eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM)

Name	Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM)
eCH-Nummer	eCH-0107
Kategorie	Standard
Reifegrad	implementiert
Version	3.0
Status	Genehmigt
Beschluss am	2018-11-28
Ausgabedatum	2019-01-14
Ersetzt Version	2.0 <Major Change>
Voraussetzungen	-
Beilagen	-
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	Fachgruppe IAM Projektgruppe SEAC Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch Marc Kunz, BFH TI, marc.kunz@bfh.ch Thomas Kessler, Temet, thomas.kessler@temet.ch Torsten Gruoner, ISB, torsten.gruoner@isb.admin.ch Marc Heerkens, ISB, marc.heerkens@isb.admin.ch eCH Fachgruppe IAM
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Das vorliegende Dokument definiert die Prinzipien, die Regeln und den Ordnungsrahmen für die IAM-Systemgestaltung, welche beim Bereitstellen von föderierten IAM-Lösungen im föderalen E-Government Schweiz berücksichtigt werden müssen. Das Gestaltungsprinzip definiert eine modellhafte IAM-Landschaft in organisationsübergreifenden Applikationsszenarien für bestehende und neue Anwendungen. Dabei wird davon ausgegangen, dass Prozesse und IAM-Services durch die Anforderungen der verschiedenen Stakeholder motiviert und durch die definierten Akteure verteilt erbracht resp. genutzt werden können. Der Standard spezifiziert die Anforderungen, die Stakeholder und Akteure, die Prozesse, die Informationsarchitektur und die IAM-Services. Des Weiteren werden Aspekte des Schutzes der Privatsphäre und die Auswirkungen der Ausdehnung des IAMs auf das Internet of Things diskutiert.
Der Standard kann in allen E-Society-Bereichen (E-Government, E-Health, E-Economy) angewendet werden.

Inhaltsverzeichnis

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

1 Status des Dokuments

Genehmigt: Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

2 Einleitung

2.1 Überblick

Die Nutzung des Internets hat in den letzten Jahren kontinuierlich zugenommen. Immer häufiger wird das Internet nicht nur als Informationsquelle, sondern auch zum Tätigen von Geschäften verwendet.

Internetbasierte Geschäftsprozesse setzen vertrauenswürdige Subjekte und damit verbundenes Wissen um die Handlungspartner voraus. Entsprechende Dienste wurden bisher erfolgreich durch die organisationsinterne Identitäts- und Zugriffsverwaltung (*Identity and Access Management, IAM*) gewährleistet. In organisationsübergreifenden Anwendungsfällen trifft das interne IAM aber auf seine Grenzen: es kann nicht oder nur durch hohen Aufwand über mehrere *Domänen* hinweg verwendet werden. Der hier vorliegende Standard definiert die Anforderungen und Grundprinzipien für die Gestaltung von *föderierten IAM-Systemen* (wird im Dokument auch IAM-System oder IAM-Gesamtsystem genannt) im E-Government, damit die genannte Grenze überwunden werden kann. Sie sind beim Bereitstellen von Lösungen im E-Government Schweiz zu berücksichtigen, damit lokale Anwendungen und Dienste organisationsübergreifend genutzt werden können. Der Standard dient als Grundlage für alle, welche im E-Government-Umfeld Lösungen entwerfen, die potentiell oder bereits aktuell für extern Zugreifende bereitgestellt werden (Internet-eServices).

Im E-Government-Umfeld geht es, wie im gesamten E-Society-Kontext (E-Government, E-Health, E-Economy), vereinfacht darum, dass *Subjekte* (Verwaltungen, Bürger, Organisationen, Firmen, spezifische Applikationen) *Ressourcen* (Services der Gemeinden, der Kantone, des Bundes oder Dritter) verwenden möchten. Eine besondere Herausforderung ist die Tatsache, dass *E-Ressourcen* und *E-Identities* sich in unterschiedlichen *Domänen* befinden können.

2.1.1 Einführung IAM

Die Kernelemente eines *IAM* sind für das Verständnis des Standards essentiell und werden daher in diesem Abschnitt kurz erläutert. Die in diesem Dokument verwendeten Begrifflichkeiten entstammen dem IAM-Glossar (eCH-0219 [1]) und sind kursiv markiert.

In der nachfolgenden Abbildung 1 werden die Kernelemente des IAM dargestellt. Im Zentrum aller IAM-Bemühungen steht, dass der Zugriff eines *Subjekts* auf eine schützenswerte *Ressource* kontrolliert erfolgt.

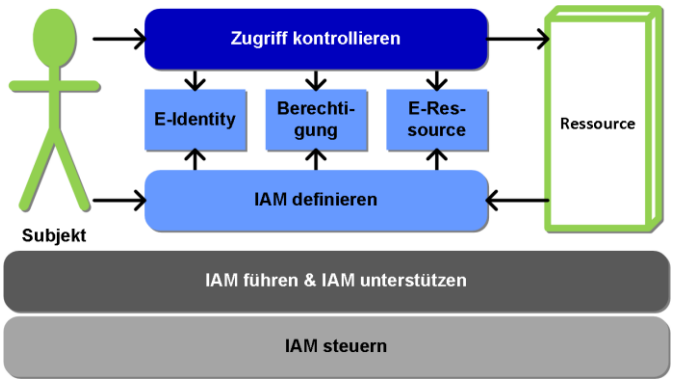


Abbildung 1 IAM im Überblick

Die Elemente *Zugriff kontrollieren* und *IAM definieren* stellen die Kernprozesse dar, welche vom *Subjekt* und der *Relying Party* genutzt werden. Diese Kernprozesse werden zu unterschiedlichen Zeitpunkten verwendet, welche durch die hellblaue und dunkelblaue Farbe (Farbverwendung siehe Tabelle 1) symbolisiert werden.

hellgrau	Hellgrau visualisiert sind in diesem Dokument für Elemente, die standardisierenden Charakter haben und Leitplanken bieten bzw. definieren.
dunkelgrau	Dunkelgrau visualisiert sind in diesem Dokument Elemente, die bereits vor der Definitionszeit und während der gesamten Lebensdauer des IAM-Systems aktiv sind (z. B. unterstützende Prozesse wie Führung oder Support).
hellblau	Die hellblaue Farbe wird in diesem Dokument konsequent für die Definitionszeit verwendet, während der alle Informationen den Informationselementen zugeordnet (also definiert) werden.
dunkelblau	Die dunkelblaue Farbe wird durchgehend für die Laufzeit verwendet. Zur Laufzeit wird der Zugriff basierend auf den definierten Informationselementen kontrolliert (gewährt oder abgelehnt).
hellgrün	Die hellgrüne Farbe wird in diesem Dokument konsequent für Realweltobjekte verwendet.

Tabelle 1 Farbverwendung im Dokument

Subjekt und *Ressource* sind Realweltobjekte, die ihre Ziele mit Hilfe der IAM-Prozesse erreichen. Das Ziel des *Subjekts* ist der Zugriff auf die gewünschte *Ressource*. Das Ziel der *Ressource* ist, sich vor unberechtigten Zugriffen auf Informationen und Services zu schützen.

Damit die Kernprozesse auch in der digitalen Welt funktionieren, werden den Objekten der Realwelt (*Subjekt*, *Ressource*) digitale Abbildungen, sogenannte Informationselemente, zugeordnet. Zum *Subjekt* (grün) wird die *E-Identity* (hellblau) und der *Ressource* (grün) die *E-Ressource* (hellblau) zugeordnet. Die *Relying Party* legt zur Umsetzung ihrer Ziele im Informationselement *Berechtigung* (*Zugangsregel/Zugriffsrecht*) fest, welche *E-Identity* unter welchen Bedingungen auf welche *Ressource* zugreifen darf.

Der Prozess *IAM steuern* umfasst alle Aktivitäten für die Definition der notwendigen Vorgaben und Rahmenbedingungen. Der Prozess *IAM führen & unterstützen* umfasst die Führung für die Implementierung und den Betrieb eines IAM-Systems, sowie Aktivitäten zum Aufnehmen, Verwalten, Verfolgen und schlussendlichen Lösen von Problemen (Support).

2.1.2 Anwendungsgebiet

Die Vision der vernetzten Verwaltung und die damit verbundenen übergreifenden Prozesse im schweizerischen E-Government bedingen eine über Organisationsgrenzen hinweggreifende *Identitäts- und Zugriffsverwaltung*. Der vorliegende Standard eCH-0107 bildet die Basis der IAM-Standardisierung. Dabei werden die Definitionen und Begriffe aus dem eCH-0122 [2], der die Architektur des E-Government Schweiz beschreibt, zu Grunde gelegt.

Der eCH-0107 definiert Grundprinzipien, Anforderungen, Prozesse und IAM-Services für die IAM-Systemgestaltung, welche beim Bereitstellen von organisationsübergreifenden IAM-Lösungen im föderalen E-Government Schweiz zu berücksichtigen sind, damit lokale Anwendungen organisationsübergreifend genutzt werden können.

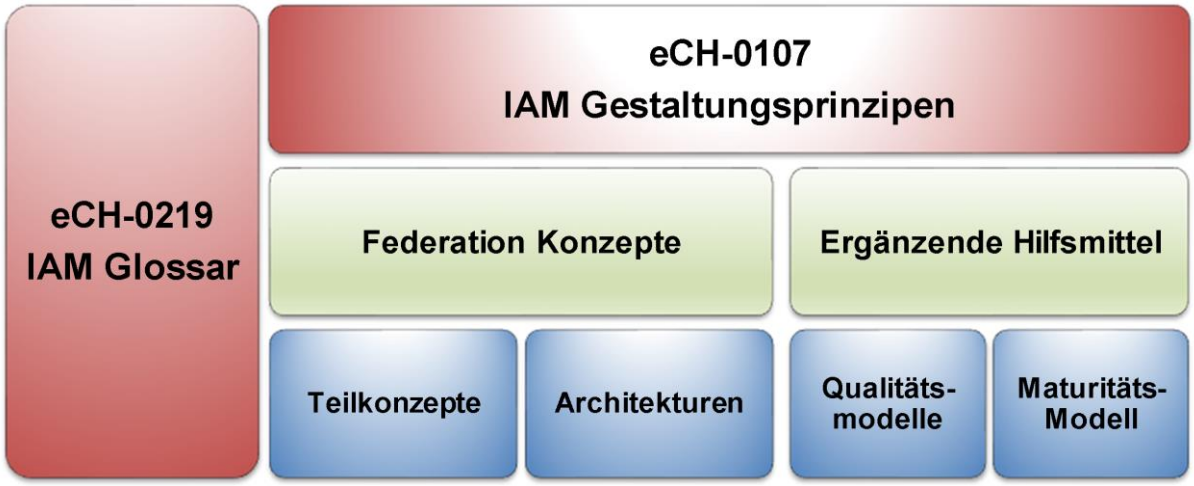


Abbildung 2 Einordnung des eCH-0107 Standards

Unter dem Standard eCH-0107 positionieren sich die Konzepte für föderierte IAM-Lösungen und ergänzende Hilfsmittel. Im IAM Glossar (eCH-0219 [1]) sind Begriffe definiert, die für alle eCH-Standards im Bereich IAM gültig sind. Die Konzepte sind konkrete Beschreibungen, wie ein IAM-Lösungsvorschlag aussieht, und beinhalten Teilkonzepte und Architekturen, die für die Umsetzung berücksichtigt werden müssen. Daneben werden den Konzepten Hilfsmittel zur Seite gestellt, die ergänzende Informationen zur Verfügung stellen und die für mehr als ein Konzept relevant sind. Die dargestellten Qualitäts- und Maturitätsmodelle sind Beispiele für Hilfsmittel und sind nicht abschliessend.

2.1.3 Föderiertes IAM

Im Unterschied zum organisationsinternen IAM geht das *föderierte IAM* von organisationsübergreifenden *E-Identities* und deren organisationsübergreifender Nutzung aus.

Die *E-Identity* für ein *Subjekt* wird in der *Domäne* A erstellt, kann aber auch Attribute aus einer *Domäne* B besitzen und zum Zugriff auf Ressourcen einer *Domäne* C verwendet werden.

Damit ein *föderiertes IAM* etabliert werden kann, müssen sich die verschiedenen *Domänen* in Bezug auf bestimmte Aspekte gegenseitig vertrauen. Dieses Vertrauen stützt sich auf explizite und implizite Vereinbarungen ab.

Beim *föderierten IAM*, im Gegensatz zum replizierenden IAM (siehe eCH-0219 [1]), im E-Government stellen Behörden den Subjekten ihren internen (andere Behörden der Schweiz) oder externen Partnern (Personen, Unternehmen, Organisationen oder Behörden anderer Staaten) Ressourcen zur Verfügung, mit denen definierte Leistungen aus dem Bereich ihrer Zuständigkeit online verfügbar gemacht werden. Diese Ressourcen sollen für Subjekte der eigenen Domäne(n) und für Subjekte mit E-Identities anderer Domänen zugreifbar sein. Eine Behörde kann somit Relying Party aber auch u.U. gleichzeitig IAM-Dienstanbieter sein.

2.1.4 Abgrenzung

Die Gestaltungsprinzipien und Regeln in diesem Standard stellen den Ordnungsrahmen für *föderierte IAM*-Systeme dar. Es werden die Kernelemente (Prozesse und IAM-Services) und die wichtigsten *Stakeholder* und *Akteure* genannt und erklärt. Ausserdem werden die verschiedenen Typologien von *föderierten IAM-Systemen* eingeführt. Die Orchestrierung und die konkrete Umsetzung der Lösungsvorschläge werden jedoch in den jeweiligen Konzepten thematisiert und in diesem Standard nicht berücksichtigt.

Generell werden in diesem Dokument nur IAM-Systeme berücksichtigt, die den *Zugriff* auf **schützenswerte Ressourcen** kontrollieren. Der *Zugriff* auf *öffentliche* oder *versteckte Ressourcen* ist nicht Teil dieses Standards.

Der im Standard verwendete Begriff *E-Identity* bezieht sich nicht nur auf die *staatlich anerkannte elektronische Identität* (*E-ID*) der Schweiz, sondern umfasst alle Arten elektronischer Identitäten, die heute üblicherweise verwendet werden (z.B. Zertifikate, Google-Accounts, SuisseID/SwissID). Zum Zeitpunkt als der Standard in der Version 3.0 überarbeitet wurde, war das E-ID Gesetz[1] in der öffentlichen Vernehmlassung und wurde daher nicht einbezogen. Sobald das E-ID Gesetz in Kraft ist, muss dieses Gesetz sowie deren Verordnung beim Aufbau und Betrieb eines IAM-Systems berücksichtigt werden.

Die Integration von *föderierten IAM-Systemen* miteinander, die sog. Interfederation, wird in diesem Standard nur erwähnt und sollte in einem eigenen Standard behandelt werden.

IAM ist eines der Mittel, um wichtige Sicherheitsziele zu erreichen. Entsprechend haben IAM-Lösungen selber die für sie geltenden, häufig hohen Sicherheitsanforderungen zu erfüllen. Diese sind in einschlägigen Sicherheitsstandards beschrieben und werden in diesem Standard nicht nochmals aufgeführt.

[1] Weitere Informationen zum E-ID Gesetz befinden sich auf folgender Webseite https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-id.html

2.1.5 Vorteile

Im Umfeld des föderierten *IAM* wurden seit der Version 1 des eCH-0107 Standards wesentliche Fortschritte erzielt, welche bereits in der zweiten Version des Standards dokumentiert und definiert wurden. Die Version 3.0 erweitert und korrigiert die Aussagen aus der zweiten Version.

Dieser Standard erzielt folgende Vorteile:

- Die Kernelemente eines *föderierten IAM-System* sind bekannt und stellen die Grundlage dar, um Lösungsideen und -vorschläge zu erarbeiten.
- Eine modellhafte *IAM*-Landschaft (Stakeholder, Akteure, Prozesse, Informationsmodell, *IAM-Services*) im organisationsübergreifenden Anwendungsszenario ist definiert.
- Die generellen Anforderungen an *föderierte IAM-Systeme* und die Anforderungen der wichtigsten Stakeholder sind definiert.
- Mögliche Konzepte für *Identity Federations* sind dargestellt.
- Die Auswirkungen auf das *IAM* bei Ausdehnung des Wirkungsbereiches auf das Internet of Things werden diskutiert.
- Verschärfte Anforderungen zum Schutz der Privatsphäre des Subjektes sind erwähnt.

2.2 Schwerpunkte

Der vorliegende Standard eCH-0107 unterteilt sich neben der Einführung in sieben Kapitel, die nachfolgend kurz beschreiben werden.

Kapitel 3 identifiziert die wichtigsten Akteure und Stakeholder sowie ihre Beziehung zueinander in einem *föderierten IAM-System*.

In Kapitel 4 werden die Grundprinzipien und die allgemeinen Anforderungen an ein *föderiertes IAM-System* sowie die Anforderungen aller Stakeholder beschrieben.

Kapitel 5 zeigt die Informationsarchitektur und erklärt die einzelnen Elemente. Mit Hilfe der Informationsarchitektur werden die Realweltobjekte über die Semantik den Schnittstellenobjekten zugeordnet.

Im Kapitel 6 werden die Prozesse definiert, welche für alle Akteure wichtig sind. Dies bedeutet, dass nicht nur die Prozesse von *IAM-Dienstanbietern* berücksichtigt werden, sondern auch die der *Relying Party* und des *Subjektes*.

In Kapitel 7 werden die *IAM-Services*, deren Schnittstellen und den Bezug zu den Prozessen in einem *föderierten IAM-System* definiert.

Kapitel 8 beschreibt die Auswirkungen auf ein IAM-System, wenn dieses auf das Internet of Things ausgeweitet wird und daher auch die *Authentifikation* und *Autorisierung* von *Dingen* mit einbezogen werden.

Kapitel 9 beschreibt Anforderungen zum Schutz der Privatsphäre des *Leistungsbezügers* (*Subjekt*), die über die Anforderungen in Kapitel 4.3.1 hinausgehen. Des Weiteren werden Richtlinien zur Verwaltung und Verarbeitung von subjektbezogenen Daten gegeben.

Kapitel 10 stellt die Varianten, ein föderiertes *IAM* aufzubauen, dar.

2.3 Normativer Charakter der Kapitel

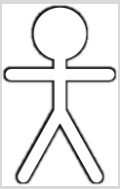
Die Kapitel des vorliegenden Standards sind von normativem oder auch deskriptivem Charakter. Die untenstehende Tabelle veranschaulicht diese Einordnung:

Kapitel	Beschreibung
1 Status des Dokuments	Deskriptiv
2 Einleitung	Deskriptiv
3 Akteure und Stakeholder	Normativ
4 Anforderungen	Normativ
5 Informationsarchitektur	Normativ
6 Prozesse	Die Benennungen und deren Definition sind normativ, die Tätigkeiten und Anmerkungen sind deskriptiv.
7 IAM-Services	Die Benennung und deren Definition sind normativ. Anmerkungen sind deskriptiv.
7.6 Zuordnung Service zu Informationselemente	Normativ
7.7 Zuständigkeiten für IAM-Services	Deskriptiv
8 IAM für das IoT	Deskriptiv
9 Privacy	Deskriptiv
10 Identity Federation Modelle	Deskriptiv
Anhang A – Referenzen & Bibliografie	Deskriptiv
Anhang B – Mitarbeiter & Überprüfung	Deskriptiv
Anhang C – Abkürzungen	Normativ
Anhang D – Glossar	Normativ
Anhang F – Änderungen gegenüber Version 2.00	Deskriptiv

Tabelle 2 Übersicht des normativen Charakters der Kapitel

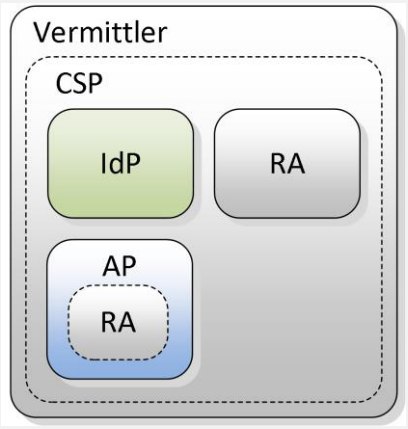
3 Akteure und Stakeholder

Ein Identity und Access Management System kennt sechs unterschiedliche Akteure, die je nach Kombination und Ausgestaltung von fünf grundlegenden Stakeholdern motiviert werden.

Akteure 	Ein Akteur beschreibt Aufgabe und Zweck einer Entität in einer Föderation und führt die Prozesse aus. Ein Akteur in einem IAM-System wird durch einen oder mehrere Stakeholder motiviert.
Stakeholder 	Die Stakeholder sind Realweltobjekte, d.h. Personen, Gruppen von Personen oder Organisationen, die gemeinsame Interessen im *IAM* haben. Ein Stakeholder hat eine (oder mehrere) Erwartung(en) (Stakes) und hat einen Willen. Stakeholder haben Anforderungen (siehe Kapitel 4) an die verschiedenen Akteure in einem IAM-System.

3.1 Akteure in IAM

Die verschiedenen Akteure, die die eigentlichen (*IAM*-)Prozesse ausführen, werden in alphabetischer Reihenfolge beschrieben. Für jeden Akteur wird zusätzlich der primäre Stakeholder (siehe Kapitel 4.3) angegeben.

IAM-Dienstanbieter	Der *IAM-Dienstanbieter* ist verantwortlich für den Betrieb[2] von einem oder mehreren IAM-Services gemäss Kapitel 7. Es können die Spezialisierungen gemäss Abbildung 3 unterschieden werden, die aber oft gemeinsam implementiert werden.  **Abbildung 3 IAM-Dienstanbieter** Die *Registrierungsstelle / Registration Authority* (*RA*) erfasst und prüft die *E-Identities* und *Attribute* der *Subjekte*. Der *Identity Provider* (*IdP*) überprüft zur *Laufzeit* die *E-Identities* der *Subjekte*. Die *Attribut Provider* (*AP*) verwaltet *Attribute* der *Subjekte* und gibt *Attributbestätigungen* aus. Der *Credential Service Provider (CSP)* vergibt und verwaltet *Authentifizierungsmittel* für *E-Identities*. Ein *CSP* enthält immer eine *RA* und umfasst die Dienste zur Überprüfung der *E-Identities* (*IdP*). Ein *Vermittler* bietet gemeinsame Dienste, wie Metadatenverwaltung, IdP-Discovery, Identity Linking oder Transformation der *Authentifizierungs-* und *Attributbestätigung*, für alle anderen *IAM-Dienstanbieter* und *Relying Parties* in einer *Identity Federation* an. Ein *Vermittler* kann optional einen *CSP* enthalten. Die Abbildung 3 stellt alle *IAM-Dienstanbieter* dar, falls sie gemeinsam implementiert werden. Primärer Stakeholder: *Dienstanbieter*

[2] Der Betrieb kann vom *IAM-Dienstanbieter* selbst gewährleistet oder auch an einem Betreiber ausgelagert werden (Outsourcing). Im Outsourcing-Fall überträgt der *IAM-Dienstanbieter* die an ihn gestellten Anforderungen an den Betreiber. Auf das IAM-Gesamtsystem hat das keinen Einfluss und wird daher in diesem Dokument nicht weiter betrachtet.

IAM-Führung	Die *IAM-Führung* ist verantwortlich für das Managen eines IAM-Systems oder von Teilen davon (*IAM-Dienstanbieter* oder *Relying Party*). Die *IAM-Führung des IAM-Gesamtsystems* managt die teilnehmenden *IAM-Dienstanbieter* und *Relying Parties* (z. B. analog zu ITIL [3]) in allen Fachbereichen wie z. B. Release-Management, Qualitätsmanagement, IAM-Lieferanten- und -Konsumentenmanagement, Service-Request-Management. Dies kann sowohl im internen Kontext als auch über Verträge/SLA mit externen *IAM-Dienstanbietern* und *Relying Parties* geschehen. Primärer Stakeholder: *Führung*
IAM-Regulator	Der *IAM-Regulator* (oder die *IAM-Steuerung*) definiert die rechtlichen, prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen, innerhalb derer das *IAM* abgewickelt werden muss. Er berücksichtigt dabei die Interessen aller Stakeholder und beteiligt alle anderen Akteure in geeigneter Weise an der Definition. *IAM-Regulatoren* existieren in verschiedenen Formen und können sowohl innerhalb einer einzigen Organisation, aber auch organisationsübergreifend agieren. Die *IAM-Steuerung* definiert die IAM-Policy für ein organisationsinternes oder -externes IAM-System bzw. von *IAM-Services*. Sie sorgt dabei auch für Orchestrierung, die strategische Weiterentwicklung und Governance des IAM-Gesamtsystems. Der *Gesetzgeber* definiert die rechtlichen Rahmenbedingungen innerhalb derer sich das IAM-Gesamtsystem bewegen und entwickeln muss. Das *Standardisierungsgremium* erstellt Normen und Richtlinien für die prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen. Primärer Stakeholder: *Regulator*
IAM-Support	Der *IAM-Support* ist verantwortlich für alle Aktivitäten zum Auffinden und Lösen von Problemen im IAM-System. Primärer Stakeholder: *Dienstanbieter*

Relying Party	Die *Relying Party* vertritt die Interessen der *Ressource* im IAM-System. Sie nutzt *IAM-Services* und verarbeitet Informationen von *IAM-Dienstanbietern* für den Schutz ihrer *Ressourcen*. Sie legt zur *Definitionszeit* über *Zugriffsrechte* und *Zugangsregeln* fest, welche *E-Identities* unter welchen Bedingungen auf ihre *Ressourcen* zugreifen dürfen. Sie braucht zur Prüfung der *Berechtigung* eines Ressourcenzugriffs zur *Laufzeit* nähere Informationen (berechtigungsrelevante Eigenschaften) zu einem *Subjekt,* dessen *E-Identity* und den Kontext des *Zugriffs* (Lokation, Zeitpunkt, *Vertrauensstufe* etc.). Primärer Stakeholder: *Leistungserbringer*

Subjekt	Eine *natürliche Person*, eine *Organisation* (*juristische Person)*, ein *Service* oder ein *Ding*, das auf eine *Ressource* zugreift oder zugreifen möchte. Ein *Subjekt* wird durch eine oder mehrere *E-Identities* repräsentiert. Primärer Stakeholder: *Leistungsbezüger*

Die Akteure können sich in verschiedenen Organisationseinheiten wiederholen. Es kommt so zu einer fachlichen Zusammenarbeit auf verschiedenen Ebenen und in verschiedenen Kontexten.

Abbildung 4 zeigt die Zusammenarbeit an einem einfachen Beispiel einer *Identity Federation* bestehend aus einer *RP* und einem *IAM-Dienstanbieter*. Es stellt eine Situation dar. Ein *Subjekt* möchte fachliche Leistungen von Organisation 1 beziehen und wird von Organisation 2 authentifiziert. Die Organisationen haben je eine *Führung* und je einen *Regulator*. Innerhalb des IAM-Gesamtsystem gibt es eine Führung und einen Regulator (Organisation 3), die das IAM-Gesamtsystem definieren. Beispiel für ein Standardisierungsgremium ist der eCH.

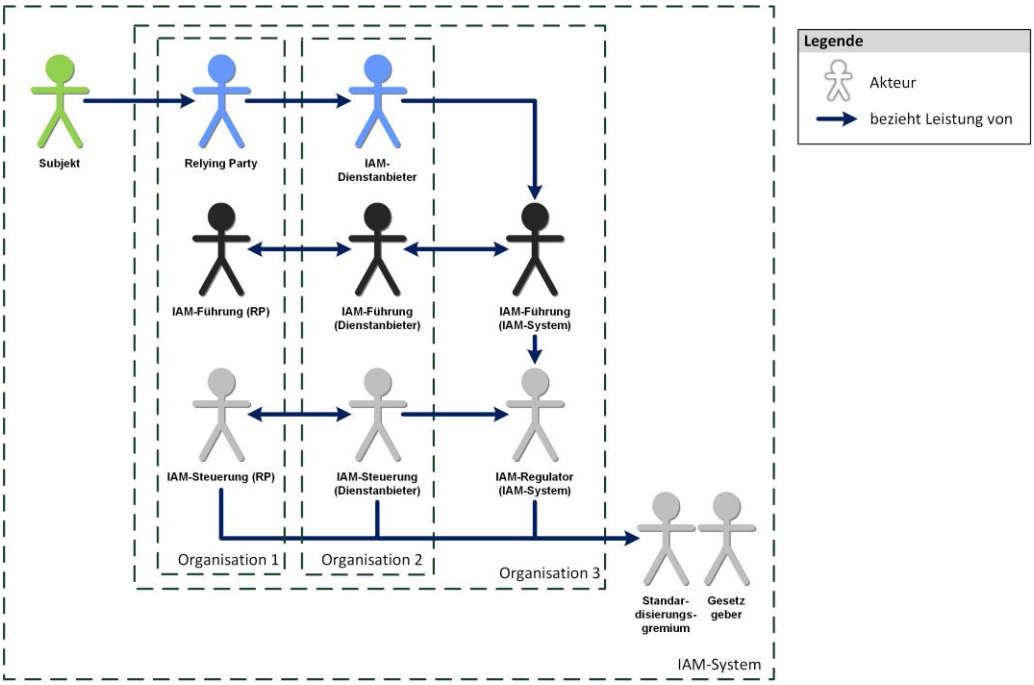


Abbildung 4 Zusammenarbeit von Akteure in einem *föderierten IAM-System*

4 Anforderungen

Die in diesem Kapitel beschriebenen und definierten Prinzipien und Anforderungen definieren und strukturieren die in Kapitel 6 modellierten Prozesse und müssen angewendet oder erfüllt werden, damit ein interoperables und effizientes *föderiertes IAM-System* aufgebaut werden kann.

Die folgenden Prinzipien und Anforderungen sind als Basis zu verstehen. Diese können als Grundlage eines zu implementierenden IAM-Systems verwendet werden und entsprechend dem Kontext und Anwendungsgebiet ergänzt bzw. angepasst werden.

Die Prinzipien und Anforderungen können in vier verschiedene Typengruppen eingeteilt werden:

- B… Business (Geschäftsanforderungen),
- D… Data (Informationen und Daten),
- A… Application (Anwendung),
- T… Technology (Technologie).

4.1 Grundprinzipien eines föderierten IAM-Systems

Die Grundprinzipien beschreiben die allgemeinen Architekturprinzipien für die Gestaltung eines *föderierten IAM-Systems*. Sie geben die Leitplanken bei der Realisierung eines *föderativen IAM-Systems* vor.

Bezeichnung	Typ	Beschreibung	Begründung
Prinzip-1	A/B	Informationen und Daten MÜSSEN föderiert statt repliziert werden, d.h. dass zur *Laufzeit* bei *Authentifizierung* und *Autorisierung* direkt auf die Daten der autoritativen Quelle zugegriffen wird, ohne dass diese als Kopie vorgehalten werden müssen.	Aktualität und Konsistenz der Daten, Kosten (Vereinfachung der Prozesse), geringere Fehleranfälligkeit
Prinzip-2	A/B	Soweit von der *Vertrauensstufe* her möglich, SOLLTEN bestehende *E-Identities*, *Authentifizierungs*- und *Attributbestätigungen* von anderen Stellen übernommen werden (Föderation).	Wiederverwendbarkeit und daraus resultierenden Effizienz
Prinzip-3	A	Für die *Authentifikation* und den *Zugang* SOLLTEN die *Relying Party* von ihr entkoppelte (IAM-)Services nutzen.	Kosten, Modularität, Erweiterbarkeit (neue Technologien)
Prinzip-4	A	Der *Autorisierung* für einen *Zugriff* auf eine schützenswerte *Ressource* MUSS die *Authentifikation* des zugreifenden *Subjekts* vorausgehen.	Feststellung der Identität des *Subjekts* als Grundlage einer Autorisierung
Prinzip-5	A/D	Zur Berechtigung SOLLTEN vorrangig regelbasierte Verfahren, die sich auf *Attribute* ab-	Antragsbasierte Verfahren bedürfen einer

Bezeich-nung	Typ	Beschreibung	Begründung
		stützen (*ABAC*), als antragsbasierte Verfahren (Genehmigung von Rollen, *RBAC*) verwendet werden.	vorgängigen Übertragung der Identität an den Berechtigungsverwalter
Prinzip-5.1	A	Der *Zugang* MUSS ausschliesslich auf Grund der angegebenen *Attribute* gewährt werden.	Unabhängigkeit der Zugangsentscheidung von Daten der Ressource, Modularität
Prinzip-6	B	Organisationsübergreifende Effektivität des IAM MUSS auf gegenseitigem spezifischem Vertrauen in die Partner basieren.	Föderation ohne Vertrauen nicht möglich
Prinzip-7	A/D	Wenn fachlich nicht notwendig, SOLLTEN keine Informationen eines zugreifenden *Subjekts*, ausser die für den Zugriffsentscheid notwendigen, an die *Ressource* weitergegeben werden.	Need-to-Know-Prinzip, Schutz der Privatsphäre
Prinzip-8	B	Die rechtlichen Rahmenbedingungen (insbesondere des Datenschutzes) MÜSSEN zu jeder Zeit gewährleistet sein. Die Einhaltung der organisatorischen, architektonischen, sicherheitsrelevanten und technischen Rahmenbedingungen SOLLTEN (sofern sie nicht in rechtlichen Rahmenbedingungen festgehalten sind) zu jeder Zeit gewährleistet sein.	Compliance, Interoperabilität
Prinzip-9	B	Das IAM SOLLTE möglichst kostengünstig, effektiv und wirtschaftlich betrieben und verwaltet werden.	Kosten
Prinzip-10	B	Um eine effektive Zusammenarbeit zu gewährleisten, SOLLTE das *IAM* auf einer international interoperablen *IAM-Architektur* basieren. [4]	Interoperabilität

4.2 Anforderungen an das föderierte IAM-System

Dieser Abschnitt beschreibt die generischen Anforderungen aller Stakeholder an ein *föderiertes IAM-System* im Schweizer E-Government.

Bezeich-nung	Typ	Beschreibung	Begründung / Prinzip
IAM-1	T/A	Das *IAM* SOLLTE auf einer international interoperablen *IAM-Architektur* basieren. [4]	Prinzip-1 Prinzip-10

Bezeich-nung	Typ	Beschreibung	Begründung / Prinzip
IAM-1.1	T/A	Das *IAM* MUSS in andere *IAM* einfach integrierbar[3] sein. Auf internationaler Ebene SOLLTE es einfach integrierbar sein.	Prinzip-10
IAM-1.2	T/A	Das *IAM* MUSS die Fähigkeit haben, bestehende IAM-Lösungen einfach zu integrieren.	Prinzip-10
IAM-2	A/D	Die *Authentifikation* und *Berechtigung* für den Zugang SOLLTEN auf **standardisierten** *Authentifizierungsmitteln* und *Attributen basieren*.	Prinzip-3 Prinzip-5.1 Prinzip-9 Prinzip-10
IAM-3	T/A	Die IAM-Systeme MÜSSEN modular und SOLLTEN skalierbar aufgebaut sein.	Wiederverwendbarkeit, Wartbarkeit Prinzip-9 Prinzip-10
IAM-4	A	Die technischen Services MÜSSEN über standardisierte Schnittstellen zusammenarbeiten, welche offene Standards gemäss ihrer Spezifikation (z. B. SAML, OIDC) benutzen.	Prinizip-10
IAM-5	T	Die je nach Schutzbedürfnissen notwendigen, unterschiedlich starken Authentisierungs- und Autorisierungsverfahren KÖNNEN auf derselben IAM-Infrastruktur realisiert werden.	Wiederverwendbarkeit Prinzip-9 Prinzip-10
IAM-6	D	Die Menge der *E-Identities*, *Authentifizierungsmittel* und *Attribute* SOLLTE minimal gehalten und womöglich konsolidiert werden.	Benutzerfreundlichkeit Prinzip-9
IAM-7	A	Der Transport der Daten MUSS zwischen den *IAM-Dienstanbietern* und *RPs* sowie den *Client Plattformen* auf Protokollebene abgesichert sein (z. B. mit TLS).	Sicherheit, Schutz der Privatsphäre Prinzip-8
IAM-8	A	Die technischen Services, welche *Authentifizierungs-* und *Attributbestätigungen* erstellen oder konsumieren, MÜSSEN ihre Zeit mit einem zugelassenen Zeitserver synchronisieren.	Sicherheit, Robustheit Prinzip-10
IAM-9	B/A	Die von den *IAM-Services* erstellten *Authentifizierungs-* und *Attributbestätigungen* MÜSSEN auf ihre Authentizität und Integrität überprüft	Sicherheit, Trust Prinzip-6

[3] Durch die Integration von IAM-Systemen können *E-Identities* über Domänengrenzen hinweg genutzt werden. Das Ziel einer solchen Integration ist die Befähigung der *Subjekte* einer *Domäne* auf die *Ressourcen* einer anderen *Domäne* zuzugreifen, ohne dass die Identitätsinformationen (*E-Identities* und zugehörige *Attribute*) mehrfach verwaltet oder repliziert werden müssen, d.h. die *E-Identities* müssen föderiert werden.

Bezeich-nung	Typ	Beschreibung	Begründung / Prinzip
		werden können (z. B. mit Hilfe der Signatur oder durch Rückfragen).	
IAM-10	A/B	Es MUSS gewährleistet sein, dass während einer angemessenen Zeitspanne nachvollzogen und nachgewiesen werden kann, welches *Subjekt* wann auf welche *Ressource* zugegriffen hat.	Nachvollziehbarkeit, Prinzip-8
IAM-11	B/A/T	Es MUSS entsprechend der Sicherheitsanforderung sichergestellt werden, dass *Authentifizierungs-* und *Attributbestätigungen* nur von berechtigten Instanzen gelesen werden können.	Schutz der Privatsphäre, Prinzip-8

4.3 Anforderungen der Stakeholder

Die Anforderungen der Stakeholder an die verschiedenen Akteure in einem IAM-System sind in Tabelle 3 überblicksmässig dargestellt. Sie werden im Folgenden einzeln aufgeführt und referenzieren sowohl die Grundprinzipien (Kap. 4.1) und Anforderungen (Kap. 4.2) eines föderierten IAM-Systems wie auch die Anforderungen anderer Stakeholder.

Rollen / **Stakeholder**	**Subjekt**	**Relying Party**	**IAM-Dienstanbieter**	**IAM-Führung**	**IAM-Support**	**IAM-Regulator**
Leistungsbezüger	X	X	X		X	X
Leistungserbringer	X		X	X	X	X
Dienstanbieter	X		X	X		X
Führung		X	X	X	X	X
Regulator				X		X

Tabelle 3 Anforderungen der Stakeholder an die Akteure

4.3.1 Leistungsbezüger (LB)

Leistungsbezüger	Der *Leistungsbezüger* möchte jederzeit, kostengünstig und einfach eine fachliche Leistung[4] online in Anspruch nehmen. Er fordert Unterstützung bei Problemen (z. B. bei Identitätsdiebstahl) und erwartet Konformität mit gesetzlichen Regelungen.

[4] Die hier erwähnte fachliche Leistung ist z. B. die Bestellung einer Funklizenz oder einer Parkkarte, nicht eine IAM-Leistung von einem IAM-Dienstanbieter.

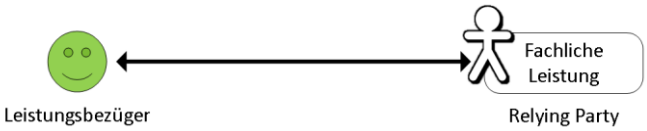


Abbildung 5: Sicht des Leistungsbezügers

Abbildung 5 zeigt die Sicht des *Leistungsbezügers* auf das IAM-Gesamtsystem. Der *Leistungsbezüger* möchte vorrangig eine fachliche Leistung einer *Relying Party* in Anspruch nehmen. Das verwendete IAM-System ist für ihn zweitrangig und nur Mittel, um sein Ziel zu erreichen.

4.3.1.1 Anforderungen des Stakeholders: Leistungsbezüger

Die Anforderungen des *Leistungsbezügers (LB)* werden von *natürlichen Personen*, *Organisationen*, Services oder *Dingen* gestellt, die auf Informationen und Services der *Ressourcen* zugreifen wollen.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
LB-1	A/D	Wenn das *Subjekt* auf eine schützenswerte *Ressource* zugreift, MUSS sich das *Subjekt* authentisieren.	*Authentifizierung* als Grundlage der *Autorisierung*, Datenschutz	**Prinzip-4**
LB-1.1	B/A/T	Das *Subjekt* MUSS sich minimal mit der geforderten *Vertrauensstufe* authentisieren. Es DARF sich mit einer höheren *Vertrauensstufe* authentisieren.	Kosten, Benutzerfreundlichkeit, Schutz der Privatsphäre	**Prinzip-7, Prinzip-5**
LB-2	D	Ein eindeutiger *Identifikator* gegenüber der *Ressource* MUSS nur dann vom *Subjekt* verwendet werden, wenn die Nutzung der *Ressource* das fordert.	Schutz der Privatsphäre	**Prinzip-7**
LB-2.1	D	Einen zufälligen *Identifikator* (z. B. eine Transient ID) gegenüber der *Ressource* SOLLTE vom *Subjekt* bei der Nutzung verwendet werden.	Schutz der Privatsphäre (Unlinkability)	**Prinzip-7**
LB-3	D	Es MÜSSEN nur die *Attribute* vom *Subjekt* bei der *Authentifikation* übermittelt werden, die zur *Berechtigung* der *Ressource* notwendig sind.	Need-to-Know-Prinzip, Schutz der Privatsphäre	**Prinzip-7**
LB-3.1	D	Weitere *Attribute* KÖNNEN vom *Subjekt* an die *Ressource* übermittelt werden.	Schutz der Privatsphäre	**Prinzip-7**

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
LB-4	B/A	Die *IAM-Dienstanbieter* (*IdP*, *AP*), welche die *E-Identities* und *Attribute* verwalten, KÖNNEN vom *Subjekt* gewählt werden.	Selbstbestimmung, Wahlfreiheit	**Prinzip-2**
LB-5	D	Die Anzahl der benötigten *E-Identities*, die das *Subjekt* haben muss, SOLLTE möglichst gering gehalten werden.	Kosten, Benutzerfreundlichkeit, Kontextabdeckung	**IAM-6**
LB-6	B	Das IAM-System SOLLTE die Möglichkeit anbieten, dass das Subjekt die Anzahl von *Authentifizierungsmittel* und *Attributen* verschiedener Qualitäten vom *Subjekt* selbst bestimmt werden.	Selbstbestimmung, Wahlfreiheit	
LB-7	B	Das IAM-System SOLLTE die Möglichkeit anbieten, dass das *Authentifizierungsmittel* (während der *Authentisierung*), welches die minimal geforderte Qualität erfüllt, vom *Subjekt* selbst bestimmt wird.	Selbstbestimmung, Wahlfreiheit	**Prinzip-2**
LB-8	B	Die Beschaffung von *E-Identities* und *Authentifizierungsmitteln* SOLLTE einfach und günstig sein.	Kosten	**Prinzip-9**
LB-9	A	Die Benutzung von *E-Identities* und *Authentifizierungsmitteln* SOLLTE einfach und unkompliziert sein.	Benutzerfreundlichkeit	
LB-10	B	Ein anderes *Subjekt* SOLL die Fähigkeit haben, kontextbezogen und zeitlich begrenzt als Stellvertreter zu handeln.	Delegation von Berechtigungen	
LB-11	B/A	Der Weitergabe von *Attributen* MUSS das *Subjekt* zustimmen können, ausser das Recht zur Weitergabe ist gesetzlich verankert oder anderswo geregelt.	Schutz der Privatsphäre	**Prinzip-8**
LB-11.1		Das Subjekt MUSS zu jederzeit die Möglichkeit haben die Freigabe zu widerrufen	Schutz der Privatsphäre	**Prinzip-8**
LB-12	B/A	Das *Subjekt* MUSS bei Vermeidung und Recovery des Missbrauchs einer *E-Identity* unterstützt werden. [4]	Benutzerfreundlichkeit, Sicherheit	**Führ-3**
LB-13	B/A/T	*IAM-Dienstanbieter MÜSSEN* das vernünftig Machbare unternehmen,	Schutz der Privatsphäre, Sicherheit	**LE-10, Führ-3**

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
		um den Missbrauch der *E-Identity* des *Subjekts* zu verhindern. [4]		
LB-14	A	Der *IAM-Support* MUSS das *Subjekt* beim Lösen von Problemen, die einen erfolgreichen Zugang/Zugriff auf die *Ressource* verhindern, unterstützen.	Benutzerfreundlichkeit	**Führ-6**
LB-15	A	Die vom *Subjekt* freigegebenen *Attribute* SOLLTEN nur von den berechtigten Instanzen gelesen werden können.	Schutz der Privatsphäre	**IAM-11**
LB-16	B	Die Nutzung der IAM-Dienste zur *Laufzeit* MUSS jederzeit möglich sein.[5]	Verfügbarkeit	
LB-17	D	Wenn die *Ressource*, auf die das *Subjekt* zugreifen möchte, subjektbezogene, sensible Daten enthält, MUSS die *RP* dafür sorgen, dass nur die berechtigten *Subjekte Zugriff* erhalten.	Schutz der Privatsphäre, Datenschutz	**Prinzip-4**

4.3.2 Leistungserbringer (LE)

Leistungserbringer	Der *Leistungserbringer* möchte fachliche Leistungen online anbieten. Dies soll kostengünstig, stabil, einfach und konform mit den gesetzlichen Regelungen sein und von möglichst vielen genutzt werden. Den *Zugriff* und den Schutz der *Ressourcen* möchte er gemäss seinen Bedürfnissen (z. B. Risikobereitschaft, Wirtschaftlichkeit) an die *IAM-Dienstanbieter* übertragen.

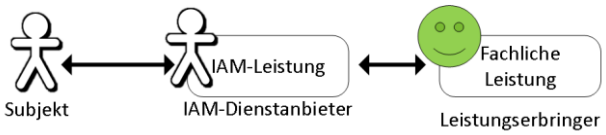


Abbildung 6 Sicht des Leistungserbringers

Abbildung 6 zeigt die Sicht des *Leistungserbringers* auf das IAM-Gesamtsystem. Der *Leistungserbringer* möchte seine fachliche Leistung dem *Subjekt* zur Verfügung stellen. Die dazu

[5] Die Ressource sollte jederzeit nutzbar sein.

notwendigen IAM-Leistung (mehrere *IAM-Services*) möchte er zumeist nicht selbst erbringen, sondern diese an *IAM-Dienstanbieter* auslagern.

4.3.2.1 Anforderungen des Stakeholders: Leistungserbringer

Dieser Abschnitt beschreibt die von den *Leistungserbringern (LE)* gestellten Anforderungen.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
LE-1	B/A/T	Der unberechtigte *Zugang/Zugriff* auf *Ressourcen* MUSS verhindert werden.	Sicherheit	
LE-2	A	Der *Zugriff* auf schützenswerte *Ressourcen* MUSS auf autorisierte *Subjekte* eingeschränkt sein.	Sicherheit (Access Control)	**Prinzip-4**
LE-2.1	A	Falls das *Subjekt* keine *Rechte* für die aufzurufende schützenswerte *Ressource* hat, MUSS der Aufruf an die *E-Ressource* verworfen und/oder entsprechend umgeleitet werden.	Sicherheit, Benutzerfreundlichkeit	
LE-3	B/A	Der Aufwand für die Verwaltung der *E-Ressourcen* SOLLTE minimal sein.	Kosten	**Prinzip-9**
LE-4	B/A	Der Aufwand für die Verwaltung der *Berechtigungen* (*Zugangsregeln* und *Zugriffsrechte*) SOLLTE minimal sein.	Kosten	**Prinzip-9**
LE-5	D	Die Menge der unterstützten *E-Identities* und *Attribute* MUSS minimal gehalten und SOLLTE womöglich konsolidiert werden.	Kosten	**Prinzip-9, IAM-6, LB-5**
LE-6	B	*E-Identities* und *Attribute* MÜSSEN bei Veränderungen zeitnah gepflegt werden.	Aktualität	
LE-7	A	*Authentifizierungs-* und *Attributbestätigungen* KÖNNEN durch *IAM-Dienstanbieter* mit unterschiedlicher Qualität ausgestellt werden. [4] Die Qualität SOLLTE integraler Teil der *Authentifizierungs-* bzw. *Attributbestätigung* sein.	Interoperabilität	**Prinzip-2**
LE-8	B	Für *Subjekte* SOLLTEN in der *Authentifizierung-* und/oder *Attributbestätigung* subjektidentifizierende *Attribute* vorhanden sein.	Wiedererkennung des Subjekts	
LE-9	B	Das *Subjekt* und die *IAM-Dienstanbieter* MÜSSEN den Verdacht	Sicherheit	

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
		eines Missbrauchs einer *E-Identity* melden. [4]		
LE-10	B/A/T	*IAM-Dienstanbieter MÜSSEN* das vernünftig Machbare unternehmen, um den Missbrauch der *E-Identity* des *Subjekts* zu verhindern. [4]	Schutz der Privatsphäre, Sicherheit	**LB-13 Führ-3**
LE-11	B/A	In einem Federation Modell mit zentralem *Vermittler* SOLLTE der *Leistungserbringer* möglichst viel Betriebsverantwortungen an den *Vermittler* delegieren.	Kosten, einfache Integration/Konfiguration, Interoperabilität	**Prinzip-9**

4.3.3 Dienstanbieter

Dienstanbieter	Der *Dienstanbieter* möchte, dass seine angebotenen IAM-Leistungen von möglichst vielen verwendet werden. Zudem strebt er eine Zusammenstellung von möglichst komplementär ausgerichteten Diensten an, um das IAM-System effizient und wirtschaftlich zu halten.

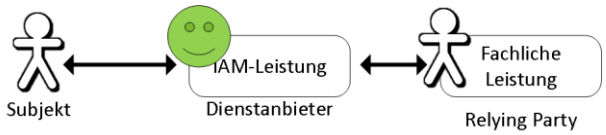


Abbildung 7 Sicht des Dienstanbieters

Abbildung 7 zeigt die Sicht des *Dienstanbieters* auf das IAM-Gesamtsystem. Der *Dienstanbieter* stellt seine IAM-Leistung der *Relying Party* und dem Subjekt zur Verfügung. Mit Hilfe dieser IAM-Leistung kann das *Subjekt* die fachliche Leistung der *Relying Party* nutzen.

4.3.3.1 Anforderungen der Dienstanbieter

Dieser Abschnitt beschreibt die Anforderungen der Dienstanbieter.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
Dienst-1	B/A	Der Aufwand für die Administration der *E-Identities* (*Authentifizierungsmittel* und *Attribute*) SOLLTE im Verhältnis zur angestrebten Qualität minimal sein.	Kosten	**Prinzip-9, LB-8**
Dienst-2	D	Der Zusammenhang zwischen der *E-Identity* und den dazugehörigen *Authentifizierungsmitteln* MUSS zu jedem Zeitpunkt gewährleistet sein.	Nachvollziehbarkeit	**IAM-10**

Bezeich-nung	Typ	Beschreibung	Begründung	Referenz
Dienst-3	B	Die *IAM-Führung* MUSS die Stabilität der prozessualen, organisatori-schen/architektonischen und techni-schen Aspekte des IAM-Systems und die Weiterentwicklung sicherstellen.	Kosten, Investi-tionsschutz	**Prinzip-9**

4.3.4 Stakeholder Führung

Führung	Die *Führung* möchte ein funktionierendes und stabiles IAM-System, das allen Stakeholdern gerecht wird. Er führt die daran beteiligten *IAM-Dienstanbietern* und *Relying Parties* und garan-tiert den zuverlässigen Betrieb des IAM-Systems.

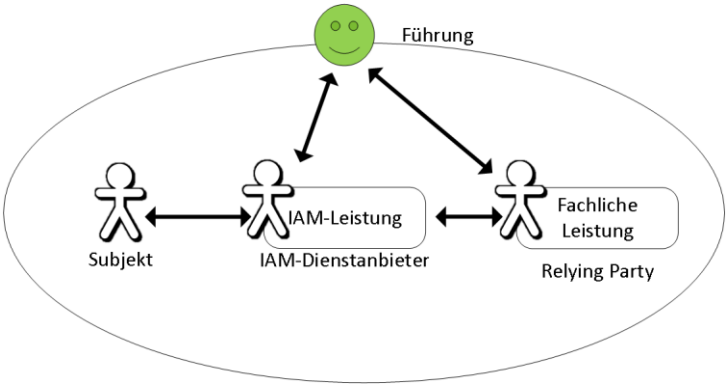


Abbildung 8 Sicht der Führung des gesamten IAM-Systems

Abbildung 8 zeigt die Sicht der *Führung* des gesamten IAM-Systems. Die *Führung* möchte das IAM-System und die daran beteiligen *Relying Parties* und *IAM-Dienstanbietern* effizient führen, um die Implementierung zu erleichtern und den zuverlässigen Betrieb zu garantieren. Die *Führung* koordiniert dabei die Anforderungen aller Stakeholder im IAM-System, auch die des *Regulators* und des *Leistungsbezügers*.

4.3.4.1 Anforderungen des Stakeholders: Führung

Dieser Abschnitt beschreibt die Anforderungen des Stakeholders *Führung*.

Bezeich-nung	Typ	Beschreibung	Begründung	Referenz
Führ-1	B/A	Die *IAM-Dienstanbieter* und *Relying Parties* SOLLTEN sich auf eine Menge von *Authentifizierungsmitteln* und *Attri-buten* einigen.	Interoperabil-ität, Be-nutzerfreun-dlichkeit, Füh-rbarkeit	**IAM-2, IAM-6, IAM-7**
Führ-2	T	Die *IAM-Dienstanbieter* und *Relying Parties* MÜSSEN standardisierte Schnittstellen verwenden.	Interoperabilität	**IAM-4**

Bezeich-nung	Typ	Beschreibung	Begründung	Referenz
Führ-3	B/A	Die verschiedenen *IAM-Dienstanbieter* und *Relying Parties* MÜSSEN zusammenarbeiten, um das *Subjekt* bei Vermeidung und Recovery des Missbrauchs seiner *E-Identity* zu unterstützen.	Benutzerfreundlichkeit, Sicherheit	**LB-12, LB-13, LE-10**
Führ-4	B/D	Die verschiedenen *IAM-Dienstanbieter* und die *Relying Parties* MÜSSEN zusammenarbeiten, so dass jederzeit nachvollzogen werden kann, welches *Subjekt* wann auf welche *Ressource* zugegriffen hat.	Nachvollziehbarkeit	**IAM-10**
Führ-5	B	Der *IAM-Regulator* MUSS die erforderlichen rechtlichen, prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen für das betroffene IAM-System definieren.	Rechtskonformität, Sicherheit, Robustheit	**Prinzip-8 Reg-1**
Führ-5.1	B	Die verschiedenen *IAM-Dienstanbieter* und die *Relying Parties* SOLLTEN die vom *IAM-Regulator* definierten Rahmenbedingungen einhalten.	Rechtskonformität, Sicherheit, Robustheit	**Prinzip-8**
Führ-6	A	Der *IAM-Support* MUSS das *Subjekt* effizient, kundenfreundlich, günstig und nachvollziehbar beim Lösen von Problemen, die einen erfolgreichen Zugang/Zugriff auf die *Ressource* verhindern, unterstützen.	Benutzerfreundlichkeit, Kosten	**LB-14**

4.3.5 Regulator

Regulator	Der *Regulator* möchte die Interoperabilität (insbesondere bei selbstständig geführten Teilsystemen), Robustheit und Sicherheit des IAM-Gesamtsystems sicherstellen.

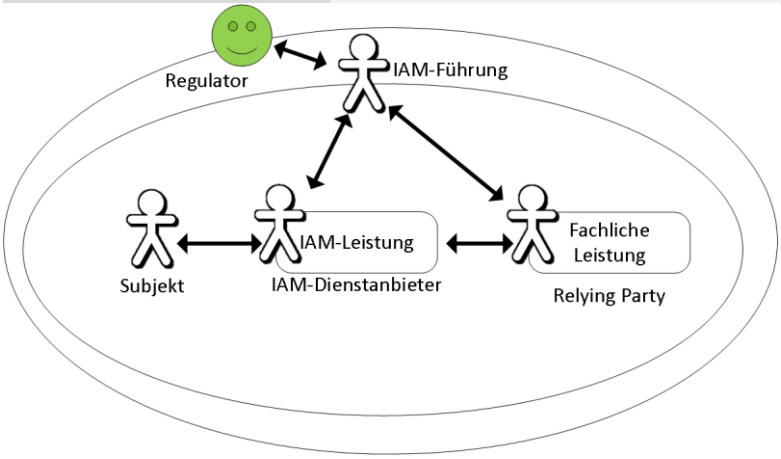


Abbildung 9 Sicht des Regulators

Abbildung 9 zeigt die Sicht des *Regulators*. Der *Regulator* möchte durch die Schaffung entsprechender Rahmenbedingungen (Gesetze, Standards, Strategien, etc.) den Einsatz von *föderierten IAM-Systemen* im organisationsübergreifenden Kontext fördern und gleichzeitig eine hohe Qualität nicht funktionaler Merkmale, wie z. B. Interoperabilität, Zuverlässigkeit und Sicherheit, erreichen.

4.3.5.1 Anforderungen des Stakeholders: Regulator

Dieser Abschnitt beschreibt die Anforderungen des Stakeholders *Regulator*.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
Reg-1	B	Die verschiedenen *IAM-Dienstanbieter* und *Relying Parties* MÜSSEN die rechtlichen Rahmenbedingungen einhalten. Die verschiedenen *IAM-Dienstanbieter* und *Relying Parties* SOLLTEN (sofern sie nicht in rechtlichen Rahmenbedingungen festgehalten sind) die definierten prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen einhalten.	Compliance, anwendbare Datenschutzgesetze und kantonale Datenschutzregeln	**Prinzip-8** **Führ-5**
Reg-2	B	Die Einhaltung der definierten rechtlichen, prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen MÜSSEN durch entsprechende Evidenzen belegt werden können.	Compliance	**Prinzip-8**
Reg-3	B	Bei Nichteinhaltung MUSS die *IAM-Führung* eine begründete Ausnahme beantragen und bewilligen lassen.	Risikomanagement	**Prinzip-8**

5 Informationsarchitektur

Nachstehendes Modell stellt die wichtigen Begriffe des *IAM* und ihre Beziehungen in einer Übersicht als UML-Klassendiagramm dar. Weil die Elemente des *IAM*-Informationsmodells an sehr vielen Orten (nicht nur im *IAM*) verwendet werden, ist es hier wichtig, differenzierte Begriffe zu verwenden, damit Syntax und Semantik für alle Beteiligten eindeutig und unmissverständlich definiert sind. Abbildung 10 zeigt das Informationsmodell zum organisationsübergreifenden *IAM*.

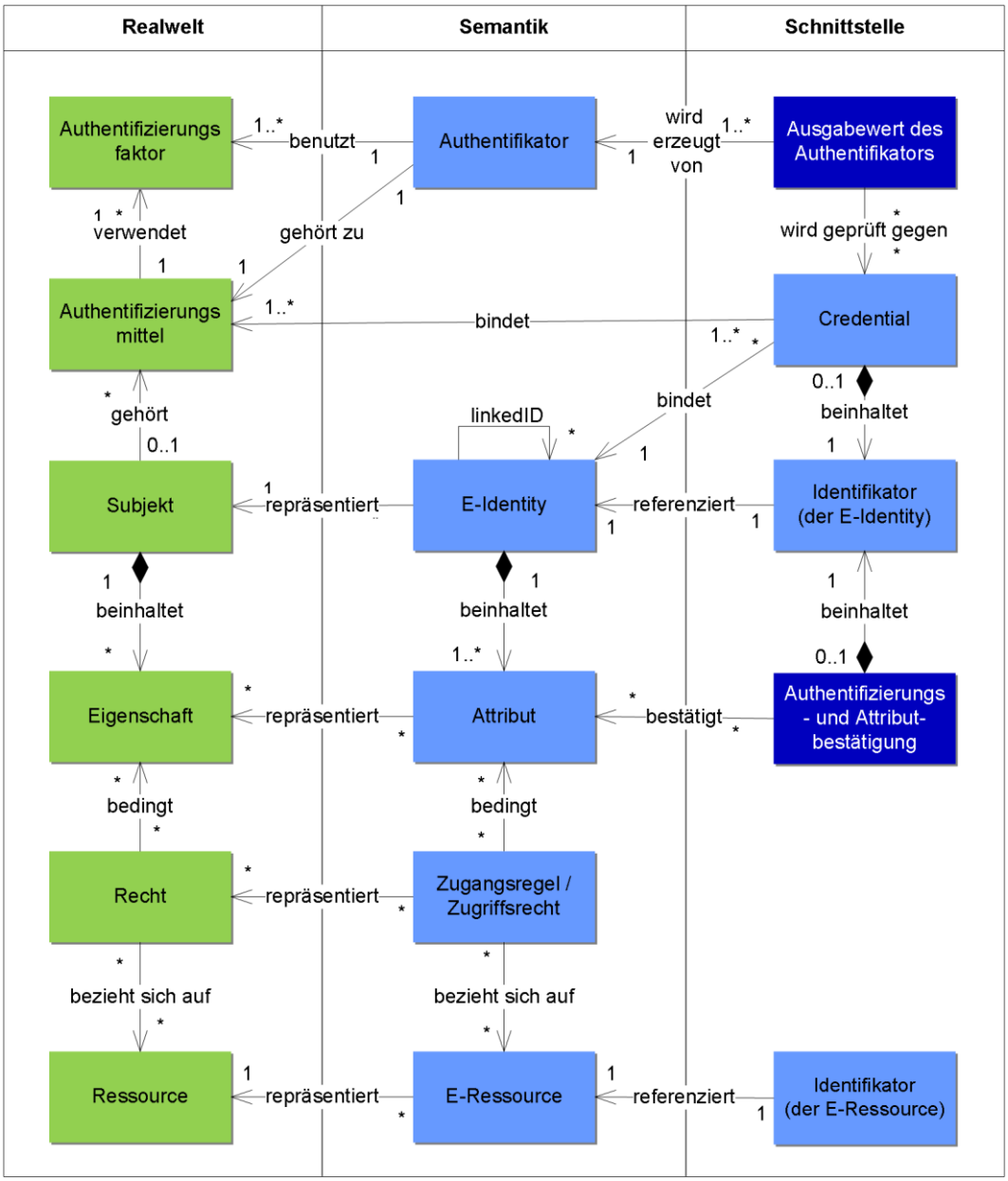


Abbildung 10 Informationsmodell

Allgemein ist es üblich, zwischen dem Fachbereich und den Informationssystemen für die Elemente der realen Welt die gleichen Bezeichner zu verwenden. Weil im *IAM* die Unterschiede zwischen der semantischen Sicht (der beteiligten Informationssysteme) und der realen Welt wesentlich sind, werden hier für unterschiedliche Elemente auch unterschiedliche Bezeichner verwendet. Das Informationsmodell in Abbildung 10 zeigt links (in grün) die Elemente der realen Welt, in der Mitte das semantische Modell (der Informationssysteme), und rechts die Schnittellenobjekte, die zum Informationsaustausch zwischen Informationssystemen verwendet werden. Objekte, die zur *Definitionszeit* entstehen, sind entspr. der Farbverwendung aus Tabelle 1 hellblau dargestellt, Objekte der *Laufzeit* in dunkelblau.

Das semantische Modell in der Mitte macht keine Aussagen über die Verteilung der Information über Informationssysteme.

Zur *Definitionszeit* (siehe Prozesse in Abschnitt 6.2 und IAM-Services in Abschnitt 7.2) werden Objekte der realen Welt mit ihren Eigenschaften und Beziehungen in die Informationssysteme (Semantik) abgebildet.

Zur *Laufzeit* (siehe Prozesse in Abschnitt 6.1 und IAM-Services in Abschnitt 7.3) werden Schnittstellenobjekte auf Basis der Inhalte des semantischen Modells erstellt und zwischen Informationssystemen ausgetauscht.

Die nachfolgende Tabelle beschreibt kurz[6] die in der Abbildung 10 vorkommenden Elemente und ihre Beziehungen.

Realwelt	
Ressource	Service oder Daten, auf welche ein *Subjekt* zugreifen kann, wenn es sich *authentisiert* hat und es auf der Basis der benötigten *Attribute autorisiert* wurde. Dies schliesst physische Ressourcen wie Gebäude und Anlagen, deren Benutzung über IT-Systeme gesteuert wird, mit ein.
Recht	Die *Rechte* sind spezifische abstrakte *Eigenschaften*, welche das *Subjekt* besitzen muss, um auf eine *Ressource* zugreifen zu dürfen. Diese können z. B. in Gesetzen oder Verträgen festgelegt sein.
Eigenschaften	*Eigenschaften* sind charakteristische Merkmale oder charakteristisches Verhalten eines *Subjekts*, die in ihrer Summe für das *Subjekt* spezifisch sind.

[6] Die vollständigen Beschreibungen mit Abbildungen und Beispielen sind im eCH-0219 [1] zu finden.

Subjekt

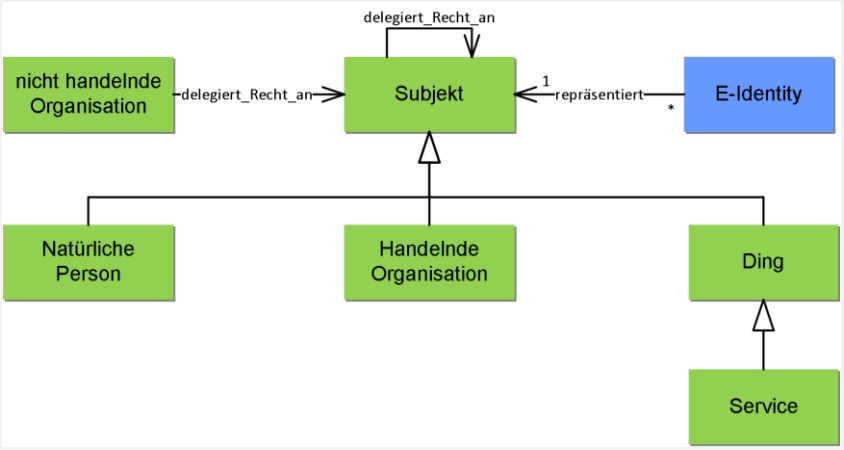


Abbildung 11 *Subjekt* Definition

Ein *Subjekt* ist eine *natürliche Person*, eine handelnde *Organisation*, ein *Service* oder ein *Ding*, das auf eine *Ressource* zugreift oder zugreifen möchte.

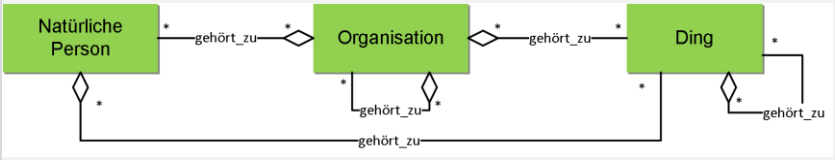
Ein *Subjekt* wird durch *E-Identities* in der digitalen Welt repräsentiert.

Ein *Subjekt* kann *Rechte* an ein weiteres *Subjekt* delegieren.

Eine *Organisation* ist eine Gruppe aus mehreren *natürlichen Personen* oder *Dingen*. Eine *Organisation* kann (Unter-)Organisationen enthalten.

Dabei wird zwischen *handelnden* und *nicht handelnden* Organisationen unterschieden. *Handelnde Organisationen* (z. B. Gruppen-Identitäten) können sich authentifizieren und *Zugriff* zu *Ressourcen* erhalten. Nicht *handelnde Organisationen* (z. B. *juristische Personen*) können sich nicht selbst authentifizieren, sondern nur über das dazugehörige *Subjekt* (z. B. eine *natürliche Person*), an das sie ihre *Rechte* delegieren.

Eine *juristische Person* ist eine spezielle *Organisation*, die von einer anerkennenden *Behörde* anerkannt wird. Die Anerkennung beruht auf einen Vertrag zwischen der anerkennenden *Behörde* und der *juristischen Person*. Einer *juristischen Person* muss immer mindestens eine *natürliche Person* zugeordnet sein.

	Ein *Ding* ist eine existierende oder abstrakte Einheit, die eindeutig identifizierbar ist.  **Abbildung 12 Zugehörigkeit der *Subjekte*** *Dinge* können weitere *Dinge* enthalten. Ein *Ding* kann zu einer *Organisation* oder zu einer *natürlichen Person* gehören. Ein *Service* ist ein spezielles *Ding*, das über ein *Netzwerk* erreichbar und darin digital identifizierbar ist.
Authentifizierungsmittel	Etwas, das ein *Subjekt* besitzt und unter seiner Kontrolle hat (ein kryptographischer Schlüssel, ein Geheimnis oder ein spezifisches Verhalten). Ein *Authentifizierungsmittel* kann einen (*single-factor authenticator*) oder auch mehrere unabhängige *Authentifizierungsfaktoren* (*multi-factor authenticator*) benutzen.
Authentifizierungsfaktor	Informationen und/oder Prozesse, die zur *Authentifizierung* eines *Subjektes* verwendet werden können. *Authentifizierungsfaktoren* können auf vier verschiedenen Merkmalen (besitzabhängig, kenntnisabhängig, inhärent oder verhaltensbasiert) oder Kombinationen davon beruhen.
Semantik	
E-Ressource	Digitale Repräsentation einer *Ressource*. Eine *E-Ressource* hat einen *Identifikator* (eindeutiger Name, oft URL/URI), welche innerhalb eines *Namensraumes* eindeutig einer *Ressource* zugewiesen werden kann.
Zugangsregel / Zugriffsrecht	Ressourcenverantwortliche definieren die *Zugangsregeln* und *Zugriffsrechte* für ihre *E-Ressourcen*. Die *Zugangsregeln* und *Zugriffsrechte* definieren die Bedingungen, unter denen ein *Subjekt* zu einer *Ressource* Zugang erhält (*Grobautorisierung*) und auf sie zugreifen darf (*Feinautorisierung*), z. B. nach erfolgreicher *Authentifizierung* und Bestätigung bestimmter *Attribute*.
Attribut	Semantisches Abbild einer einem *Subjekt* zugeordneten *Eigenschaft*, die das *Subjekt* näher beschreibt. Der *Identifikator* ist ebenfalls ein speziell verwendetes *Attribut*.

E-Identity	Repräsentation eines *Subjekts*. Eine *E-Identity* (*digitale Identität*) hat einen *Identifikator* (eindeutiger Name), meist zusammen mit einer Menge von zusätzlichen *Attributen*, welche innerhalb eines *Namensraumes* (und damit einer *Domäne*) eindeutig einem *Subjekt* zugewiesen werden können. Ein *Subjekt* kann mehrere *E-Identities* haben.[7]
linkedID (Relation)	Im organisationsübergreifenden Kontext erlaubt die Relation *linkedID*, *E-Identities* aus verschiedenen *Domänen* miteinander in Beziehung zu setzen. *E-Identities* können mit *linkedIDs* zu einem beliebigen gerichteten Graphen verkettet werden. Die konkrete Umsetzung von eCH-0107 kann die Form zusätzlich einschränken (z. B. statt Graph nur Baumstruktur) und regelt entsprechend ihrer Fähigkeiten die Interpretation (Semantik) des Graphen. (vgl. 7.3.4 *Broker Service*).
Authentifikator	Funktionales Abbild des *Authentifizierungsmittels* der Realwelt. Mit der Funktion eines *Authentifikators* wird aus einem Eingabewert und einem geheimen Wert ein Ausgabewert erzeugt.
Schnittstelle	
Authentifizierungs- und Attributbestätigung	Eine Bestätigung der erfolgreichen *Authentifikation* eines *Subjektes* (*Authentifizierungsbestätigung*) oder eine Bestätigung eines Wertes eines *Attributs* (*Attributbestätigung*). Enthält einen *Identifikator*.
Identifikator	Eine Zeichenkette, welche eine *E-Identity* oder eine *E-Ressource* innerhalb eines *Namensraumes (Domäne)* eindeutig bezeichnet.
Credential	Stellt eine Menge von Daten dar, mit der eine *E-Identity* an ein *Authentifizierungsmittel* gebunden wird, welches vom *Subjekt* besessen und kontrolliert wird.
Ausgabewert des Authentifikators	Wird durch eine mathematische Funktion (*Authentifikator* oder Authentifizierungsfunktion) aus einem geheimen Wert (z. B. privater Schlüssel), einem oder mehreren optionalen Aktivierungswerten (z. B. PIN oder biometrischer Informationen), und einem oder mehreren optionalen Eingabewerten (z. B. Zufallswerten oder Challenges) generiert. Der Ausgabewert des Authentifikators ist so stark wie das verwendete Verfahren bzw. dessen Implementation.

Tabelle 4 Beschreibung der Elemente des Informationsmodels

[7] Die Aussage gilt (im Rahmen von eCH-0107) für organisationsübergreifende Systeme. Es wird allerdings empfohlen, bezüglich Eindeutigkeit auch organisationsintern keine Einschränkungen zu machen.

6 Prozesse

Abbildung 13 zeigt eine Übersicht über die Geschäftsprozesse. Sie dient zur Veranschaulichung der Tätigkeiten, welche für eine erfolgreiche Kooperation zwischen den Akteure in einem IAM-System (siehe Definitionen in Kapitel 3.1) notwendig sind. Die blau dargestellten Prozesse bilden die Kernprozesse, die grau dargestellten bilden die Führungs- und Steuerungsprozesse.

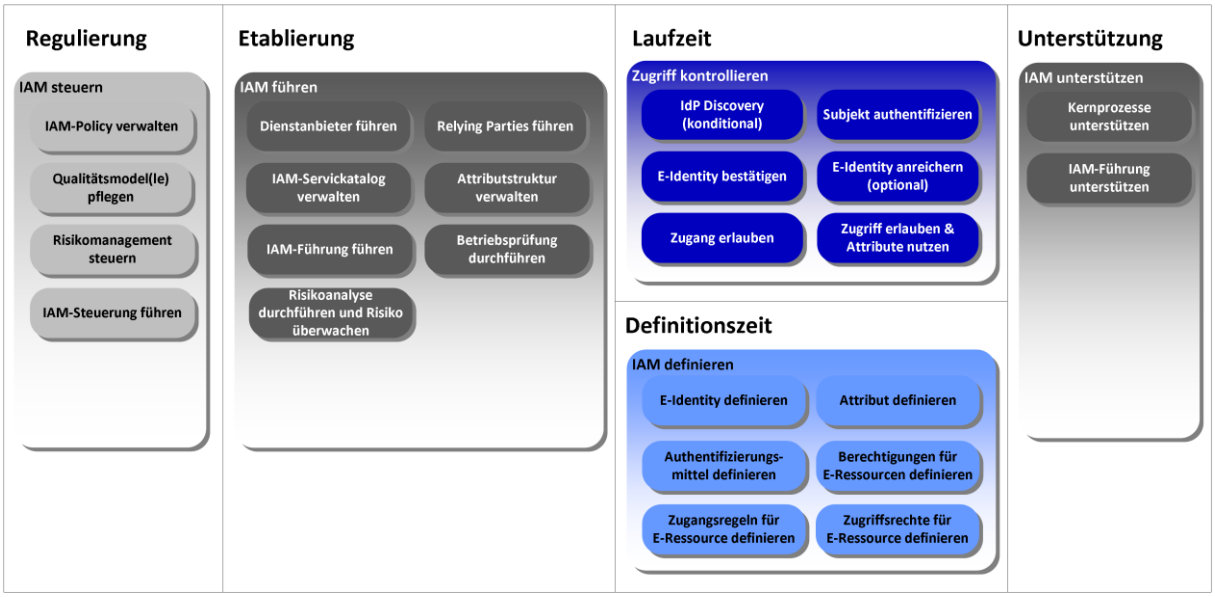


Abbildung 13 IAM-Prozesslandkarte

An diesen Prozessen beteiligen sich die verschiedenen Akteure gemäss Kapitel 3.1. Die nachstehenden Abschnitte beschreiben die Geschäftsprozesse mit ihren Teilprozessen.

Der erwähnte Prozesseigner ist typischerweise der Akteur, welcher die Verantwortung für den Prozess trägt. Die *Führung* bestimmt und orchestriert aber auf Grund der Architektur und Topologie die Zugehörigkeit der Prozesse zu den Akteuren.

Die Tätigkeiten sind zum Teil als ‘konditional’ oder ‘optional’ gekennzeichnet. ‘konditional’ bedeutet, dass die Tätigkeit vom Resultat einer anderen Tätigkeit oder einer ‘optionalen’ Tätigkeit abhängig ist. ‘optional’ gekennzeichnete Tätigkeiten können je nach definierter *IAM-Architektur* und/oder *IAM-Policy* ausgeführt werden.

6.1 Zugriff kontrollieren (Laufzeit)

Zugriff kontrollieren umfasst die Prozesse der *Laufzeit*. Ziel von *Zugriff kontrollieren* ist die kontrollierte und garantierte Einhaltung der Regeln für den *Zugriff* eines *Subjekts* auf eine *Ressource*. Beim *Zugriff* des *Subjekts* wird dieses *authentifiziert* und schliesslich, sofern berechtigt, *autorisiert*, auf die *Ressource* zuzugreifen. In einem *föderierten IAM-System*, in dem der *Identity Provider* und die Relying Party über ein *Netzwerk* getrennte Systeme sind, muss die bei der *Authentifizierung* bestätigte *E-Identity* des *Subjekts* zusätzlich föderiert werden.

Die Teilprozesse von *Zugriff kontrollieren* bauen in einer festgelegten Reihenfolge aufeinander auf (siehe Abbildung 14).

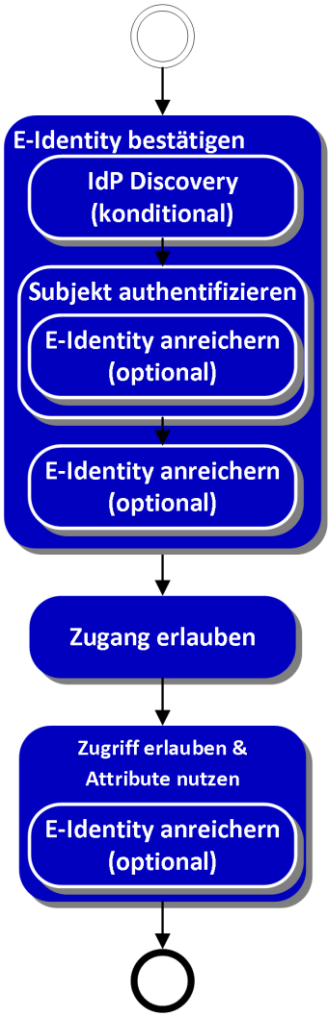


Abbildung 14 Ablaufdiagramm *Zugriff kontrollieren*

Im Sinne einer zuverlässigen Informationsbereitstellung stellt *Zugriff kontrollieren* sicher, dass nur genau diejenigen *Subjekte* auf die *Ressource Zugriff* erhalten, die *Zugriff* haben dürfen. Allen andern wird der *Zugriff* auf die *Ressource* oder bereits der *Zugang* zur *Ressource* verweigert.

Die IAM-Services, die die Schnittstellen zu den Prozessen zur Laufzeit definieren, sind im Abschnitt 7.3 beschrieben.

6.1.1 E-Identity bestätigen

E-Identity bestätigen	Erzeugen und übergeben der Bestätigung der *E-Identity* durch den *IdP* oder *Vermittler* an die *RP*.

Prozesseigner: *RP* oder *Vermittler* (*IAM-Führung* bestimmt und orchestriert die Zuständigkeiten)

Anforderungen: LB-2, LB-2.1, LB-13, LB-16, LE-2, LE-8, LE-10, Führ-3

Beim Prozess *E-Identity bestätigen* wird je nach verwendetem Identity Federation Modell (siehe auch Kapitel 10 Identity Federation Modelle) von einem anderen Akteur übernommen:

Tätigkeiten:

RP-zentriertes Modell oder Federation Modelle mit *Vermittler* (siehe Kapitel 10):

- (optional bei *Vermittler*) Überprüfen, ob die *RP* berechtigt ist, eine *Authentifizierungsbestätigung* anzufordern. Falls die Überprüfung erfolgreich ist, ist die *RP* berechtigt, *Authentifizierungsbestätigungen* zu erhalten. Falls die Überprüfung erfolglos ist, ist die *RP* nicht berechtigt und der Prozess wird abgebrochen.
- (konditional) Falls das *Subjekt* gemäss *IAM-Policy* bei mehreren *IdPs* authentifizieren kann wird der Prozesse *IdP Discovery* (6.1.2) angestossen.
- Der Prozess *Subjekt authentifizieren* (6.1.3) wird angestossen.
    - (optional bei *Vermittler*) Gemäss den *linkedID*-Beziehungen, wird einmal (oder mehrmals) der Prozess *Subjekt authentifizieren* (6.1.3) bei weiteren *IdPs* angestossen (*Identity Mapping*).
- (optional) Holt das Einverständnis des *Subjekts* ein, die *Authentifizierungsbestätigung* an den aufrufenden Service zu übermitteln. Falls das *Subjekt* das Einverständnis nicht gibt, wird der Prozess abgebrochen.
- Erzeugt eine *Authentifizierungsbestätigung* mit Zeitstempel, Signatur, *Identifikator* (gemäss Anforderungen *RP*, *Subjekt* und *IAM-Policy*) und optionaler Verschlüsselung.
- (optional) Einen *AP* wählen, welche in der *Definitionszeit* mit der *E-Identity* verlinkt wurde.
- (optional) *E-Identity anreichern* (6.1.4) anstossen.
    - (optional bei *Vermittler*) Der *Vermittler* kann *E-Identity anreichern* (6.1.4) mehrmals ausführen und die *Attribute* aggregieren.
    - (optional bei *Vermittler*) Der *Vermittler* transformiert die *Attribute* gemäss der *IAM-Führung* erstellten Richtlinien.
- (optional bei *Vermittler*) Der *Vermittler* transformiert die Protokolle gemäss der *IAM-Führung* erstellten Richtlinien
- Die *Authentifizierungsbestätigung* wird an den Prozess *Zugang erlauben* (6.1.5) übergeben.
    - (konditional) Falls der Prozess *E-Identity anreichern* (6.1.4) angestossen wurde, wird die *Attributbestätigung* an den Prozess *Zugang erlauben* (6.1.5) übergeben.
- Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).

IdP/AP-zentriertes Modell (siehe Kapitel 10.2):

- Der Prozess *Subjekt authentifizieren* (6.1.3) wird angestossen.
- Erzeugt eine *Authentifizierungsbestätigung* mit Zeitstempel, Signatur, *Identifikator* (gemäss Anforderungen *RP*, *Subjekt* und *IAM-Policy*) und optionaler Verschlüsselung.

- (optional) Einen *AP* wählen, welche in der *Definitionszeit* mit der *E-Identity* verlinkt wurde.
- (optional) *E-Identity anreichern* (6.1.4) anstossen; ggf. mehrmals ausführen und die *Attribute* aggregieren.
- (optional) Transformieren der Protokolle gemäss der *IAM-Führung* erstellten Richtlinien.
- Es wird eine Auswahl an *RPs zur* Verfügung gestellt, von welcher das *Subjekt* einen wählen kann.
- (optional) Holt das Einverständnis des *Subjekts* ein, dass die *Authentifizierungsbestätigung* und/oder *Attributbestätigung* an den ausgewählten *RP* übermittelt wird. Falls das *Subjekt* das Einverständnis nicht gibt, wird der Prozess abgebrochen.
- Die *Authentifizierungsbestätigung* und/oder *Attributbestätigung* wird an den Prozess *Zugang erlauben* (6.1.5) übergeben.
- Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).

Anmerkungen:

Falls der *IdP* und *AP* auf dieselbe Instanz fällt, wird dies als IdP/AP bezeichnet. In diesem Fall wird normalerweise die *Authentifizierungs-* und *Attributbestätigungen* vom IdP/AP erzeugt und beantworten.

6.1.2 IdP Discovery (konditional)

IdP Discovery	Bereitstellung einer Auswahl von *IdPs* für das *Subjekt*.

Prozesseigner: *RP* oder *Vermittler*

Anforderungen: LB-1.1, LB-7, LB-16, LE-10, Führ-3

Tätigkeiten:

- Es wird eine Auswahl an *IdPs* zur Verfügung gestellt, von welcher das *Subjekt* einen wählen kann.
    - (optional) Die Wahl des *IdP* kann anhand von persönlichen Präferenzen gespeichert werden, so dass nicht bei jedem *Zugriff* eine erneute Auswahl erforderlich ist.
- Das *Subjekt* wählt einen *IdP* aus, von welchem er überzeugt ist, dass er sich authentifizieren kann.
    - (optional) Allenfalls dem *Subjekt* Entscheidungshilfe anbieten oder bei der Auswahl des *IdP* unterstützen und ev. den Prozess *Kernprozesse unterstützen* (6.5.1) anstossen.
    - (konditional) Falls das *Subjekt* noch nicht registriert ist, wird der Prozess *E-Identity definieren* (6.2.1) angestossen.

6.1.3 Subjekt authentifizieren

Subjekt authentifizieren	Vorgang der zeitnahen Überprüfung einer behaupteten *E-Identity* eines *Subjekts* durch einen *Identity Provider*.

Prozesseigner: *IdP*

Anforderungen: LB-1, LB-9, LB-13, LB-16, LE-10, Führ-3

Tätigkeiten:

- Überprüfen, ob der aufrufende Service berechtigt ist, eine *Authentifizierung* zu veranlassen.
- Das *Subjekt* verwendet ein ihm zur Verfügung gestelltes und unter seiner Kontrolle befindliches *Authentifizierungsmittel*. (Credential Discovery)
- Das *Authentifizierungsmittel* generiert mit Hilfe des *Authentifikators* einen Ausgabewert aus den Eingaben des *Subjekts*. Das *Authentifizierungsmittel* übergibt den generierten Ausgabewert an einen *Verifier* zur Überprüfung.
- Der *Verifier* prüft den generierten Ausgabewert vom Authentifikator mit dem *Credential* der behaupteten *E-Identity*. Ist die Prüfung positiv, ist die *Authentifizierung* erfolgreich und das *Subjekt* ist authentifiziert. Ist die Prüfung negativ, ist die *Authentifizierung* erfolglos und das *Subjekt* ist nicht authentifiziert.
- (optional) Holt das Einverständnis des *Subjekts* (Einschränkung auf natürliche Personen) ein, die *Authentifizierungsbestätigung* zu übermitteln.
- (IdP mit integralem AP – IdP/AP) *E-Identity anreichern* (6.1.4) anstossen.
- (optional) Etabliert eine zeitlich befristete sichere Verbindung zur *Client Plattform* des *Subjekts* (z. B. Browser oder App).
- (optional) Kann die *Authentifizierungsbestätigung* an den aufrufenden Service übermitteln, so lange die sichere Verbindung zur *Client Plattform* des *Subjekts* besteht (unterstützt Single Sign-On).

6.1.4 E-Identity anreichern (optional)

E-Identity anreichern	Anreichern von *Attributen* zu der entsprechenden *E-Identity*.

Prozesseigner: AP

Anforderungen: LB-11, LB-13, LB-15, LB-16, LE-8, LE-10, Führ-3

Tätigkeiten:

- Der *AP* überprüft, ob der aufrufende Service berechtigt ist, eine *Attributbestätigung* anzufordern. Falls die Überprüfung erfolgreich ist, ist der aufrufende Service berechtigt *Attributbestätigung* zu erhalten. Falls die Überprüfung erfolglos ist, werden die *Attributwerte* nicht übermittelt und/oder eine Fehlermeldung/Exception wird übergeben.
- Der *AP* bereitet die entsprechenden *Attribute* auf. Berechnete und abgeleitete *Attributwerte* aus *Attributen* (z. B. over18) können generiert werden.

- (konditional) Bei Mehrfachwerten von *Attributen* wählt das *Subjekt* einen entsprechenden *Attributwert* aus.
- (konditional) Der *AP* holt das Einverständnis des *Subjekts* ein, die *Attributbestätigung* an den aufrufenden Service zu übermitteln. Falls das *Subjekt* das Einverständnis gibt, wird die *Attributbestätigung* übermittelt. Falls das *Subjekt* das Einverständnis nicht gibt, werden die *Attributwerte* nicht übermittelt und/oder eine Fehlermeldung/Exception wird übergeben.
- Der *AP* erzeugt eine *Attributbestätigung* mit Zeitstempel, Signatur, *Identifikator* (gemäss Anforderungen aufrufender Service, *Subjekt* und *IAM-Policy*) und optionaler Verschlüsselung.
- Der *AP* bestätigt elektronisch mit entsprechender Qualität (siehe z. B. Qualitätsmodell zur Attributbestätigung eCH-0171 [5]), ob ein bestimmtes *Attribut* einem *Subjekt* zugewiesen ist oder nicht.
- (optional) Der *AP* kann die *Attributbestätigung* für den aufrufenden Service (oder den End-Empfänger) verschlüsseln.
- Der *AP* übergibt die *Attributbestätigung* an den aufrufenden Service.
- Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).

Anmerkungen:

Der *AP* kann integraler Bestandteil von einem *IdP* sein. In diesem Fall spricht man von einem IdP/AP.

6.1.5 Zugang erlauben

Zugang erlauben	*Grobautorisierung* anhand der *Zugangsregeln*.

Prozesseigner: Vermittler oder RP

Anforderungen: LB-13, LB-16, LE-1, LE-10, Führ-3

Beim Prozess *Zugang erlauben* wird je nach verwendetem Identity Federation Modell (siehe auch Kapitel 10) von einem anderen Akteur durchgeführt.

Tätigkeiten:

- Vorbedingung einer *Grobautorisierung* ist die erfolgreiche *Authentifizierung* des *Subjekts*.
- Ermitteln der *Zugangsregeln* für den *Zugang* auf die *E-Ressource.*
- Überprüfen, ob der *Zugang* anhand der geforderten *Authentifizierung* und die geforderten *Attribute* in der gewünschten Qualität für das *Subjekt* autorisiert ist. Ist die Überprüfung positiv, wird der *Zugang* erlaubt. Falls die Überprüfung negativ ist, hat das *Subjekt* keinen Zugang.
- Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).

- Gibt die *Authentifizierungsbestätigungen* und die *Attributbestätigungen* weiter und stösst den Prozess *Zugriff erlauben und Attribute nutzen* (6.1.6) an.

6.1.6 Zugriff erlauben und Attribute nutzen

Zugriff erlauben und Attribute offenlegen	Prüfen der *Zugriffsberechtigung* einer *grobautorisierten E-Identity* auf eine *E-Ressource* und Erteilen des *Zugriffs* auf eine E-*Ressource* zur *Laufzeit*. Offenlegen von *Attributen* des *Subjektes*.

Prozesseigner: RP

Anforderungen: LB-3, LB-3.1, LB-16, LE-1, LE-2, LE-2.1, LE-8

Tätigkeiten:

- Vorbedingung für einen *Zugriff* ist eine erfolgreiche *Grobautorisierung*.
- Die *RP* überprüft die Aktualität und Authentizität der *Authentifizierungsbestätigung*. Ist die Überprüfung positiv, ist die *Authentifizierung* erfolgreich und das *Subjekt* ist authentifiziert. Falls die Überprüfung fehlschlägt, ist das *Subjekt* nicht authentifiziert und der *Zugriff* wird verweigert.
- Die *RP* überprüft die Aktualität und Authentizität der erhaltenen *Attributbestätigung*. Ist die Überprüfung positiv, sind die *Attributwerte* gültig und aktuell. Falls die Überprüfung fehlschlägt, ist es in der Verantwortung der *RP* entsprechend zu reagieren.
- Die *RP* ermittelt die *Zugriffsrechte* für den *Zugriff* auf die *E-Ressource*. Daraus werden die benötigten *Attributwerte* zur *E-Identity* abgeleitet.
- Die *RP* überprüft, ob die benötigten *Attributwerte* (auch für die Erfüllung ihrer fachlichen Funktion) vorhanden sind.
    - (konditional) Der Prozesseigner wählt einen *AP*, welche in der *Definitionszeit* zu der mit der *E-Identity* in Verbindung gebracht wurde.
    - (konditional) Teilprozess *E-Identity anreichern* (6.1.4) anstossen.
- Sind die benötigten *Attributwerte* vorhanden, erlaubt die *RP* den *Zugriff*. Das *Subjekt* greift anschliessend auf die *Ressource* zu. Falls die benötigten *Attributwerte* nicht vorhanden sind, so ist das *Subjekt* nicht zugriffsberechtigt und erhält eine entsprechende Fehlermeldung.
- Erzeugt ein Security Token für das autorisierte *Subjekt* mit den im Zugriffskontext relevanten und bestätigten *Attributen*.
- Begrenzt die Lebensdauer des Security Tokens.
- In Abhängigkeit der verlangten *Vertrauensstufe* muss die *RP* das *Subjekt* nach einer bestimmten Zeitdauer (unabhängig von ihren eigenen Richtlinien) erneut durch den *IdP* authentifizieren lassen (Re-Authentifizierung).
- (optional) Arbeitet mit dem Lizenzmanagement zusammen, z. B. um den *Zugriff* zu verweigern, wenn die maximale Anzahl von gleichzeitigen Benutzern erreicht ist.

- Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).

6.2 IAM definieren (Definitionszeit)

Während der *Definitionszeit* werden alle notwendigen Bedingungen geschaffen, damit zur *Laufzeit* bestimmt werden kann, ob ein *Subjekt* auf eine schützenswerte *Ressource* zugreifen darf. Die Abläufe der *Definitionszeit* müssen stattfinden, bevor *das Subjekt* die *Ressource* benutzt. Die Qualität von *Zugriff kontrollieren* wird sehr direkt durch die Umsetzung von *IAM definieren* beeinflusst.

IAM definieren besteht aus zwei unterschiedlichen Teilprozessen, die unabhängig voneinander ablaufen können (siehe Abbildung 15).

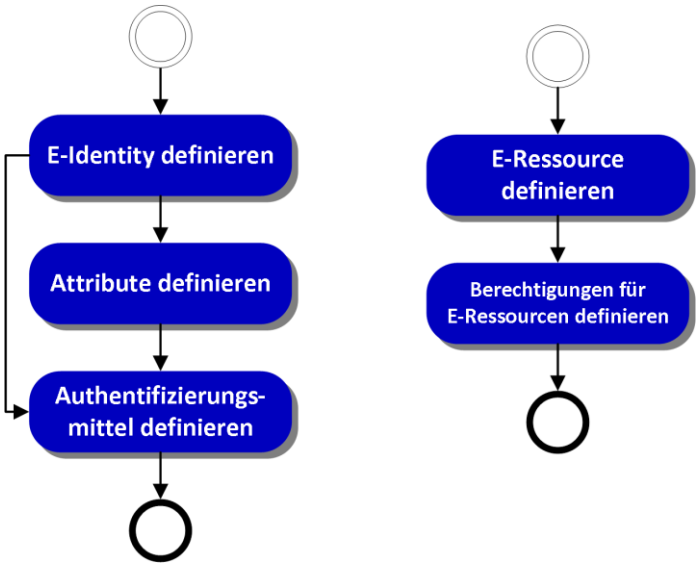


Abbildung 15 Ablaufdiagramme *IAM definieren* (Links: Definieren einer E-Identity; Rechts: Definieren einer E-Ressource)

Die *IAM-Services*, die die Schnittstellen zu den Prozessen der *Definitionszeit* definieren, werden im Abschnitt 7.2 genauer beschrieben.

6.2.1 E-Identity definieren

E-Identity definieren	Umfasst Ausgabe, Pflege und Verwaltung von *E-Identities* und deren Beziehungen und Sicherstellung der Qualität und Aktualität der *E-Identities*.

Prozesseigner: *RA*

Anforderungen: LB-4, LB-5, LB-8, LB-9, LB-10, LE-5, LE-6, Dienst-1

Tätigkeiten:

- (optional) Das *Subjekt* wählt die *RA* aus der durch die *IAM-Führung* (6.3.1 Dienstanbieter führen) definierten Menge aus.

- (optional) Das *Subjekt* wird gemäss der gewünschten *Vertrauensstufe* durch die *RA* identifiziert und seine *Beweismittel* verifiziert. Ist die Überprüfung positiv, registriert die *RA* die zugehörige *E-Identity.* Falls die Überprüfung negativ ist, kann die *E-Identity* nicht mit der gewünschten *Vertrauensstufe* registriert werden.
    - Bei Selbstregistrierung (die vom *Subjekt* erfassten *Attribute* werden nur minimal überprüft) kann die Vorlage von *Beweismitteln* und deren Überprüfung entfallen. *Attribute* können selbstdeklariert sein.
- (konditional) Möchte das *Subjekt* eine *juristische Person* vertreten, muss die *RA* die Bindung zur *juristischen Person* anhand von *Beweismitteln* verifizieren. Bei erfolgreiche Überprüfung werden entsprechende *Attributwerte* beantragt.
- (optional) Die *RA* erhebt Daten, um die Anwesenheit des *Subjekts* bei der Registrierung zu einem späteren Zeitpunkt beweisen zu können.
- Bei Selbstregistrierung (*Subjekt* registriert sich selbst) kann die Vorlage von *Beweismitteln* und deren Überprüfung entfallen. *Attribute* können selbstdeklariert sein.
- Begrenzt die Lebensdauer von *E-Identities* und unterstützt die *Subjekte* bei der Erneuerung ihrer *E-Identities*.
- (optional) Verlinken von *E-Identities* (*Identity Linking*).
- Aktualisieren (z. B. bei Step-Up Registrierung) und deaktivieren von *E-Identities*. Dafür werden die nächsten Prozesse angestossen (*Attribute definieren* (6.2.2) und *Authentifizierungsmittel definieren* (6.2.3)).
- Unterstützt *Profile* zur Trennung von Verantwortungen (Segregation of Duties, SoD).
- Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).

Anmerkungen:

Die *E-Identity* ist das zentrale Element in jedem *IAM*-System. Ein registriertes *Subjekt* hat innerhalb einer *Domäne* immer mindestens eine *E-Identity*.

6.2.2 Attribute definieren

Attribute definieren	Erfassen, Aktualisierung und Löschung von *Attributwerten*.

Prozesseigner: *AP*

Anforderungen: LB-6, LE-5, LE-6, Dienst-1, Führ-1

Tätigkeiten:

- Vorbedingung zum Definieren von *Attributwerten* ist eine vorhandene *E-Identity* (*E-Identity definieren* 6.2.1), der die *Attributwerte* zugewiesen werden können.

- Das *Subjekt* oder die *RA* des *CSPs* beantragt während der (Selbst-)Registrierung einen neuen *Attributwert* oder die Aktualisierung eines bestehenden *Attributwertes* beim *AP*. Die *RA* ist für die Überprüfung der *Attributwerte* zuständig.
- (optional) Die *RA* des *AP* erhebt *Attributwerte* gemäss der gewünschten Qualitätsstufe.
- Stellt in geeigneter Weise die Aktualität der *Attributwerte* sicher (kann z. B. deren Lebensdauer beschränken)
- (nur *RBAC*) Die *RA* kann dem *Subjekt* (Rollen-)*Attributwerte* zuweisen, die dem Subjekt vom Berechtigungsverwalter zugeteilt wurden (*RBAC*/antragsbasiertes Verfahren). Ein entsprechender *Attributwert* wird beantragt.
- (optional) Das *Subjekt* kann seine *Rechte* zeitlich begrenzt und kontextbezogen an ein anderes *Subjekt* übertragen.
- Der *AP* teilt der *E-Identity* den *Attributwert* zu oder aktualisiert ihn. Dabei werden die Attributdefinitionen vom Prozess *Attributstruktur verwalten* (6.3.3) verwendet.
- Der *AP* löscht ggf. *Attributwerte*.
- Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).

Anmerkungen:

Attribute beschreiben immer die zugehörige *E-Identity*, können aber durch den gemeinsamen Kontext von *Subjekten* (z. B. gemeinsamer Arbeitgeber) gegeben sein. Diese *Attribute* sind in der Pflege vom Lifecycle der *E-Identity* unabhängig. Nur die Beziehung der *E-Identity* zu diesen *Attributen* hängt vom Lifecycle der *E-Identity* ab.

Je nach Organisation und *Identity Federation* Modell kann die *RA* für die *CSP* und *AP* dieselbe sein. Die *IAM-Führung* bestimmt wie die Verantwortungen aufgeteilt werden.

Ein *Attributwert* repräsentiert eine einem *Subjekt* zugeordnete *Eigenschaft*, die das *Subjekt* näher beschreibt. Der Prozess, wie diese *Eigenschaften* zu erheben und prüfen sind, muss entsprechend der verlangten Qualität dokumentiert werden.

6.2.3 Authentifizierungsmittel definieren

Authentifizierungsmittel definieren	Erstellen, Vergabe und Erneuerung von *Authentifizierungsmitteln* für eine *E-Identity.*

Prozesseigner: *CSP*

Anforderungen: LB-6, LB-8, LB-9, Dienst-1, Dienst-2, Führ-1

Tätigkeiten:

- Vorbedingung ist eine vorhandene *E-Identity* (*E-Identity definieren* 6.2.1), der die *Authentifizierungsmittel* zugewiesen werden können.

- Der *CSP* erstellt, erhebt und vergibt *Authentifizierungsmerkmale* (z. B. Passwörter, Authentisierungszertifikat) oder bindet *Authentifizierungsmittel* an die *E-Identity* des *Subjektes*, die bereits unter Kontrolle des *Subjektes* sind. Eines oder mehrere *Credentials* werden erstellt und an das *Authentifizierungsmittel* gebunden.
- Der *CSP* stellt die Vertraulichkeit, Integrität und Verfügbarkeit der *Credentials* sicher.
- Die *Credentials* werden dem Prozess *Subjekt authentifizieren* (6.1.3) zur Verfügung gestellt.
- (optional) Der *CSP* verwendet für kryptografische Schlüssel ein Schlüsselmanagement.
- (optional) Der *CSP* publiziert die öffentlichen Elemente der *Authentifizierungsmittel* (z. B. öffentlicher Schlüssel) zur *E-Identity*.
- Der *CSP* händigt das *Authentifizierungsmittel* (ev. mehrere) gemäss gewünschter Vertrauensstufe an das *Subjekt* aus.
- Der *CSP* erneuert bzw. ersetzt benutzerfreundlich *Authentifizierungsmittel*.
- Der *CSP* revoziert *Authentifizierungsmittel*.
- Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).

6.2.4 E-Ressource definieren

E-Ressource definieren	Identifikation, Registrierung und Löschen von *E-Ressourcen*.

Prozesseigner: *IAM-Führung* (*RP*)

Anforderungen: LB-16, LE-1, LE-3

Tätigkeiten:

- Die *IAM-Führung* (*RP*) identifiziert *Ressourcen* und registriert die zugehörige *E-Ressource* (mit *Identifikator*). Eine *Ressource* kann durch mehrere *E-Ressourcen* repräsentiert sein.
- (optional) Die *IAM-Führung* (*RP*) klassifiziert *E-Ressourcen* entsprechend ihres Schutzbedarfes bezüglich Vertraulichkeit, Integrität und Verfügbarkeit
- Die *IAM-Führung* (*RP*) löscht oder deaktiviert die *E-Ressource*, sowie dessen *Identifikator*. Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).

Anmerkungen:

- Eine *Relying Party* hat innerhalb einer *Domäne* immer mindestens eine *E-Ressource*.

6.2.5 Zugangsregeln für E-Ressourcen definieren

Berechtigungen für E-Ressourcen definieren	Zuweisen, Aktualisieren und Löschen von *Zugangsregeln* zur *Grobautorisierung* und *Zugriffsrechten* zur *Feinautorisierung* der *E-Identities* für den *Zugriff* auf *Ressourcen*.

Prozesseigner: *RP* oder *Vermittler*

Anforderungen: LB-17, LE-1, LE-4

Tätigkeiten:

- Verwalten von *Zugangsregeln* unter Verwendung der verfügbaren *Attribute* von *E-Identities,* Kontext des Zugangs (Lokation, Zeitpunkt, *Vertrauensstufe* usw.).
- Zuweisen von *Zugangsregeln* zu einer oder mehreren *E-Ressourcen*.
- Aktualisieren und Löschen von *Zugangsregeln.*
- Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).
- (optional) Greift in den *Zugangsregeln* auch auf den Schutzbedarf der angeforderten *Ressource* (z. B. Klassifizierungsstufe) sowie Kontextinformationen (z. B. Bedrohungslage) zu.

6.2.6 Zugriffsrechte für E-Ressourcen definieren

Berechtigungen für E-Ressourcen definieren	Zuweisen, Aktualisieren und Löschen von *Zugriffsrechten* zur *Feinautorisierung* der *E-Identities* für den Zugriff auf *Ressourcen*.

Prozesseigner: *RP*

Anforderungen: LB-17, LE-1, LE-2, LE-2.1, LE-4

Tätigkeiten:

- Die *RP* verwaltet *Zugriffsrechte* unter Verwendung der verfügbaren *Attribute* von *E-Identities,* Kontext des Zugriffs (Lokation, Zeitpunkt, *Vertrauensstufe* usw.) und optional eigenen Daten.
- Die *RP* weist *Zugriffsrechte* zu einer oder mehreren *E-Ressourcen* zu.
- Die *RP* aktualisiert und löscht *Zugriffsrechte.*
- Es werden alle Aktionen und getroffenen Entscheidungen registriert und dokumentiert (Logging).

6.3 IAM führen (Etablierung)

Der Geschäftsprozess *IAM führen* beinhaltet, unter Berücksichtigung der Rahmenbedingungen der *IAM-Steuerung* und nur innerhalb eines organisatorischen Kontextes, die notwendigen Aktivitäten für die Erreichung der definierten *IAM* Ziele, die Etablierung und Verwaltung

der (ausführenden) Geschäftsprozesse und der „Roadmap“ für die Weiterentwicklung des IAM-Systems.

Diese Prozesse beschreiben die Abläufe für die Definition der notwendigen Vorgaben und Rahmenbedingungen für den Betrieb des IAM-Systems, wie z. B. das Definieren des Angebots, das Definieren der Regeln und Abläufe, dem Festlegen der Revision der Ausführung etc.

6.3.1 Dienstanbieter führen

Dienstanbieter führen	Beziehungsaufnahme, -pflege und -beendung mit den *IAM-Dienstanbietern* des IAM-Systems inkl. der Etablierung der Vertrauensbeziehungen

Prozesseigner: *IAM-Führung* (IAM-Gesamtsystem)

Anforderungen: Führ-5, Führ-5.1, Reg-1

Tätigkeiten:

- Definieren, welche *IAM-Dienstanbieter* (*IdP*, *AP*, *CSP*, *RA*, *Vermittler*) in den Verbund aufgenommen werden.
- *IAM-Dienstanbieter* in den Verbund aufnehmen und entfernen (z. B. wegen End-Of-Life oder Nichteinhalten der Sicherheitsvorgaben).
- Vertrags- und/oder SLA Management mit den verschiedenen *IAM-Dienstanbietern* oder Akzeptanz der geltenden AGBs von *IAM-Dienstanbietern*.
- Festlegung der *IAM-Organisation* (Rollen) sowie ihrer Beziehung untereinander (Zusammenarbeit).
- (konditional) Falls die IAM-Steuerung im Prozess *IAM-Policy verwalten* (6.4.1) den Vertrauensanker nicht festgelegt hat, muss der Vertrauensanker über die Auswahl der Certificate Authority (CA) festgelegt werden.
- Bestimmen und Nachführen der *Vertrauensstufen* für die *Authentifizierung*.
- (Optional) Bestimmen und Nachführen der Qualitätsstufen der *Attribute*.
- Auswirkungsanalyse von Änderungen an den Vertrauensbeziehungen.

6.3.2 Relying Parties führen

Relying Parties führen	Beziehungsaufnahme, -pflege und -beendung mit den *Relying Parties (RP)* inkl. der Etablierung der Vertrauensbeziehungen.

Prozesseigner: *IAM-Führung* (IAM-Gesamtsystem)

Anforderungen: Führ-5, Führ-5.1, Reg-1

Tätigkeiten:

- Aufnahme von *RPs* prüfen, z. B. Erfüllung der Sicherheitsanforderungen basierend auf dem Schutzbedarf prüfen.
- Vertrags- und/oder SLA-Management mit den *RPs*.
- *RPs* in den Verbund aufnehmen und entfernen (z. B. wegen End-Of-Life, Weiterentwicklung der *E-Ressource* oder Nichteinhalten der Sicherheitsvorgaben). Prozess *E-Ressource definieren* (6.2.4) anstossen.
- Prüfen der notwendigen *Attribute* (Vorhandensein und Qualität) und allenfalls Prozess *Attributstruktur verwalten* (6.3.3) anstossen.
- Auswirkungsanalyse vor Änderungen an den Vertrauensbeziehungen.
- (Optional) Im Fall, dass es mehrere *Domänen* gibt, Zugehörigkeit bestimmen.

6.3.3 Attributstruktur verwalten

Attributstruktur verwalten	Definition und Weiterentwicklung der Attributdefinition.

Prozesseigner: *IAM-Führung* (Gesamtsystem) und *IAM-Führung* (AP)

Anforderungen: LE-7, Führ-1

Tätigkeiten:

- Attributquellen suchen und prüfen.
- (konditional) Falls keine Attributquelle vorhanden ist, muss der Prozess für *Attributwertbestätigung* entsprechend der gewünschten Qualitätsstufe definiert werden.
- Meta-Attribute und Semantik definieren, harmonisieren und nachführen.
- *Attribute* klassifizieren (Bsp. Persönliche- und Enterprise-Attribute).

6.3.4 Betriebsprüfung durchführen

Betriebsprüfung durchführen	Prüfen der korrekten Umsetzung und Betriebes des IAM-Systems.

Prozesseigner: *IAM-Führung*

Anforderungen: Reg-1, Reg-2

Tätigkeiten:

- Auditieren und kontrollieren der Umsetzung der Vorgaben, Qualitätsanforderungen, Regeln und Regularien.
- Reporting aller relevanten Aktivitäten.

- Massnahmen zur Verbesserungen definieren und/oder Prozesse *IAM-Führung führen* (6.3.7) anstossen.

6.3.5 IAM-Servicekatalog verwalten

IAM-Servicekatalog verwalten	Erstellen und Pflegen des IAM-Servicekatalogs

Prozesseigner: *IAM-Führung* (Gesamtsystem) und *IAM-Führung* (*Dienstanbieter*)

Anforderungen: Dienst-3

Tätigkeiten:

- Definieren der IAM-Service-Strategie.
- Definieren und Nachführen des Service-Katalogs und die zu realisierenden *IAM-Architekturen*.
- Marktanalyse für das Betreiben der Services (intern und extern)
- Roadmap für die Weiterentwicklung der *IAM-Services*.
- Informationsaustausch und Kommunikation mit den *Relying Parties*.
- Sicherstellen der Finanzierung für den Betrieb und für die Weiterentwicklung.
- Abwickeln von Weiterentwicklungs-Anfragen und allenfalls Prozess *IAM-Führung führen* (6.3.7) anstossen.

6.3.6 Risikoanalyse durchführen und Risiko überwachen

Risikoanalyse durchführen und Risiko überwachen	Durchführen von Risikoanalyse und Risikobeurteilung. Definieren von risiko-mitigierenden Massnahmen und Risiko-Überwachung. Festhalten der Resultate.

Prozesseigner: *IAM-Führung*

Anforderungen: Reg-1, Reg-3

Tätigkeiten:

- Durchführen von Risikoanalysen und Festhalten der Resultate, damit Gefahren zeitnah erkannt werden können.
- Risikobeurteilung und Schutzbedarfsanalyse des IAM-Systems: Die Schutzbedarfsanalyse gewährleistet angepasste Sicherheitsanforderungen (so viel Sicherheit wie nötig, nicht so viel wie möglich).
- Risiko-mitigierende Massnahmen definieren und auslösen.
- Implementieren des Informations- und Datenschutzkonzepts, sowie Feedback an *IAM-Regulator* bezüglich des Informations- und Datenschutzkonzeptes.

- (Optional) Abstützung des Risikomanagements auf ein Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001, ISM3[8] oder nach ISO 31000 [6]. Abstützung des Risikomanagements auf ein Framework wie COBIT [7].
- Abstimmung mit dem *IAM-Regulator*.

6.3.7 IAM-Führung führen

IAM Führung führen	Festlegung der Zusammenarbeit der (*IAM-*)*Führungen* im IAM-Gesamtsystem.

Prozesseigner: *IAM-Führung* (IAM-Gesamtsystem)

Anforderungen: Dienst-3, Führ-5

Tätigkeiten:

- Festlegung der Zusammenarbeit der *IAM-Führungen* im IAM-Gesamtsystem.
- Definition und kontinuierliche Verbesserung der Kern-, Support- und Führungsprozesse.
- Erstellen und Bereitstellen von stufengerechten Kommunikationsmittel für diverse Stakeholder.
- Bestimmen des Zeitservers.
- Definieren, Aktualisieren und Widerrufen der Vertrauensbeziehungen (Trust) zwischen *IAM-Dienstanbietern* und *Relying Parties*. Festlegen, wie die Qualität- und Vertrauensstufen zwischen IdP/AP (oder *Vermittler*) und *RP* übermittelt werden.
- Zertifizieren von *CSPs*.
- Pflegen und Vermitteln der Metadaten zu den *IAM-Dienstanbietern* und *RPs*.
- Führung der internen *IAM-Dienstanbieter*.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.

6.4 IAM steuern (Regulierung)

Der Geschäftsprozess *IAM steuern* beinhaltet, unter Berücksichtigung der organisatorischen Rahmenbedingungen und nur innerhalb eines organisatorischen Kontexts, die notwendigen Aktivitäten für die Definition der *IAM* Ziele, der notwendigen Rahmenbedingungen und die Masterplanung für die Führung des IAM-Gesamtsystems.

Diese Prozesse beschreiben die Abläufe für die Definition der notwendigen Vorgaben und Rahmenbedingungen für die *Führung* des IAM-Systems, wie z. B. das Definieren der Regeln und standardisierten Abläufe, dem Festlegen der Revision der *Führung* etc.

[8] ISM3 ist eine ISMS komplett auf ISO 27001 abbildbar, nimmt aber zusätzlich die Maturität der Organisation in Betracht.

6.4.1 IAM-Policy verwalten

IAM Policy verwalten	Festlegung der *IAM-Policy* und der *IAM-Architektur* des IAM-Systems.

Prozesseigner: *IAM-Regulator*

Anforderungen: Führ-2, Reg-2, LE-11

Tätigkeiten:

- Ableiten und Nachführen der IAM-Strategie.
- Definieren der *IAM-Architektur*.
- Definition der *Akteure* mit entsprechenden Aufgaben, Kompetenzen und Verantwortung.
- Erarbeiten der notwendigen Basiskonzepte basierend auf den *IAM-Architekturen*, z. B. Identitätstypenkonzept und Rechtetypenkonzept.
- Erarbeiten und aktualisieren der relevanten Vorgaben: Identifikation der geltenden gesetzlichen, unternehmensinternen und vertraglichen Richtlinien / Regularien.
- Definieren und Nachführen von Hilfsmitteln für die Anwendung der IAM-Architekturen und Vorgaben. Bsp. Vertrauensstufen-Rechner.
- Definition der Nachvollziehbarkeitsanforderungen, z. B. das Ablegen der relevanten Dokumente und die Aufbewahrungsfristen der relevanten Daten (siehe auch ISO 29115 [8] Kapitel „Record-keeping/recording).
- Definieren der relevanten standardisierten Kern-, Support- und Führungsprozessen. Spezialisierung zu diesem Dokument.
- (optional) Festlegen der Vertrauensanker über die Auswahl der Certificate Authority (CA). Dies kann an die *IAM-Führung* delegiert werden.
- Festlegen des Lebenszyklus von *E-Identities*, *Attributen*, *Berechtigungen*, *IAM-Dienstanbietern* und *RPs*.
- (konditional) Festlegen des Lebenszyklus einer Verknüpfung von *natürlichen* und *juristischen Personen* (z. B. Aktivierung, Aussetzung, Erneuerung, Widerruf) (siehe auch eIDAS 2015/1502 [9], Abschnitt 2.1.4).
- (Optional) Maturitätsmodell und Maturitätsstufen festlegen (z. B. nach eCH-0172 [10]).
- Erstellen eines Verfahrens, welche die Definition und Einhaltung der Richtlinien für die Teilnehmer einer Gemeinschaft gewährleistet (z. B. Baseline Requirements, Practice Statement und Compliance Report).
- Überprüfen, ob die Richtlinien eingehalten werden. Ausnahmen, die die *IAM-Führung* beantragt, überprüfen.

6.4.2 Qualitätsmodel(le) pflegen

Qualitätsmodel(le) pflegen	Festlegen, wie die Qualität der *Authentifizierung* eines *Subjektes* und die Qualität der *Attribute* bestimmt, überprüft und verglichen werden kann.

Prozesseigner: *IAM-Regulator*

Anforderungen: Prinzip-5, IAM-1, LE-7, Reg-2

Tätigkeiten:

- Qualitätsmodell für die *Authentifizierung* von *Subjekten*, dessen Kriterien und dessen Unterteilung definieren (z. B. nach eCH-0170 [11]).
- Falls es *Attribute* gibt, sollte das Qualitätsmodell der *Attributwertbestätigungen*, dessen Kriterien und dessen Unterteilung definiert werden (z. B. nach eCH-0171 [5]).
- (Optional) Die Interoperabilität zwischen den Qualitätsmodellen festlegen.

6.4.3 Risikomanagement steuern

Risikomanagement steuern	Kontext etablieren und Identifizieren der Risiken. Welche Risiken müssen bei der Etablierung, *Definitionszeit*, *Laufzeit* und der Unterstützung beachtet werden? Leitplanken für die *IAM-Führung*, welche Risiken gemanagt werden müssen.

Prozesseigner: *IAM-Regulator*

Anforderungen: Führ-5, Reg-1, Reg-3

Tätigkeiten:

- Definieren der IAM-Sicherheitsziele
- Kontext etablieren; Die Festlegung des Kontexts definiert den Umfang des Risikomanagementprozesses und legt die Kriterien fest, anhand derer die Risiken bewertet werden.
- Definieren, wie viel Risiko die Organisation bereit ist zu nehmen (Risikobereitschaft) und wie viel Risiko die Organisation nehmen kann (Risikotoleranz)
- Risikoidentifikation durchführen, z. B. nach ISO 31000 [6]. Überprüfung der wichtigsten organisatorischen Risikokategorien, die bei der Festlegung des Kontexts berücksichtigt wurden, Erstellung einer Übersicht mit potenziellen Risiken, die sich auf das Unternehmen auswirken können.
- Abgleich und Integration mit dem Organisationsrisikomanagementsystem und Ziele.
- Erstellung des Informations- und Datenschutzkonzepts (inkl. Hilfsmittel) für die Implementierung durch die *IAM-Führung*.

- Analyse der Risikoberichte der *IAM-Führung* und Freigabe dieser Berichte.
- Kontinuierliche Verbesserung des Informations- und Datenschutzkonzepts, z. B. analog ISO 27001 [12]. Aufgrund der Ist-Situation werden periodisch Verbesserungsmöglichkeiten identifiziert, allenfalls basierend auf der Risikobereitschaft Massnahmen geplant, umgesetzt und überprüft.
- Überwachen von bekannten/publizierten externen Sicherheitsvorfälle und Risikobeurteilungsaufträge an die *IAM-Führung*(en) erteilen.
- (Optional) Abstützung des Risikomanagements auf ein Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001, O-ISM3[8] oder nach ISO 31000 [6] Abstützung des Risikomanagements auf ein Framework wie COBIT [7].

6.4.4 IAM-Steuerung führen

IAM-Steuerung führen	Integration der IAM-Steuerung im IAM-Gesamtsystem und die Definition und kontinuierliche Verbesserung der IAM-Steuerungsprozesse.

Prozesseigner: IAM-Steuerung

Anforderungen: Führ-5

Tätigkeiten:

- Identifikation / Festlegung der Zusammenarbeit von *Steuerungs- und Führungsdomänen*: Bei der Föderation erfolgt *IAM* in der Regel über mehrere *Domänen*. Die Organisation und Abläufe zwischen den *Domänen* sind klar zu regeln.
- Veränderungen in den Regulatorien und Vorgaben verfolgen und allfällige, daraus resultierende Massnahmen identifizieren.
- Bestimmung der Methoden, Notationen, externen Standards und Frameworks, die im IAM-Gesamtsystem anzuwenden sind.
- Interoperabilität im IAM-Gesamtsystem, bezüglich Methoden, Notationen, usw. gewährleisten.
- Kontinuierliche Verbesserung von *IAM steuern*. Aufgrund der Ist-Situation werden periodisch Verbesserungsmöglichkeiten identifiziert, allenfalls basierend auf der Risikobereitschaft Massnahmen geplant, umgesetzt und überprüft.
- Unterstützende / befähigende Aufgaben (Intern / Rahmenbedingungen) ausführen, wie z. B. Konventionen für Dokumentation der *IAM-Policy* festlegen und Abgleich mit den Organisationskonventionen.

6.5 IAM unterstützen

Der Geschäftsprozess *IAM unterstützen* beinhaltet, unter Berücksichtigung der organisatorischen Rahmenbedingungen und nur innerhalb eines organisatorischen Kontexts, die notwendigen Aktivitäten für die Unterstützung, Aufbau und Betrieb eines IAM-Systems. Dies sind zusätzliche Prozesse, welche in den Kern- und Führungsprozess nicht vorhanden sind.

6.5.1 Kernprozesse unterstützen

Kernprozesse unterstützen	Der Prozess *Kernprozesse unterstützen* umschliesst die Aktivitäten zum Aufnehmen, Verwalten, Verfolgen und schliesslich Lösen von Problemen, die zur *Lauf-* oder *Definitionszeit* auftreten können.

Prozesseigner: *IAM-Support*

Anforderungen: LB-12, LB-14, LE-9, Führ-4, Führ-6

Tätigkeiten:

- Annahme und Bearbeitung von Problemfällen in Interaktion zwischen *Subjekt*, *Ressource* und allen beteiligten *Dienstanbietern*.
- Einrichten und Betrieb eines Monitoring- (zur Überwachung von Ereignissen, z. B. Serviceausfall) und Tracking-Systems zur Bearbeitung und Nachvollziehen von Problemfällen.
- Unterstützung und Einleiten von Massnahmen im Falle eines sicherheitsrelevanten Ereignisses (z. B. Cyberangriff).
- Unterstützung bei Verdacht auf Missbrauch einer *E-Identity*.
- Gewährleisten der Interoperabilität von mehreren Monitoring- und Tracking-Systemen.
- Integrieren Support-Prozessen anderer *IAM-Dienstanbieter*.

6.5.2 Führungsprozesse unterstützen

Führungsunter unterstützen	Der Prozess *Führungsprozesse unterstützen* umschliesst die Aktivitäten für die Unterstützung und Beratung der *IAM-Führung* während der Etablierung.

Prozesseigner: IAM-Support (Regulator)

Anforderungen: Führ-4

Tätigkeiten:

- Kommunikation und Schulung der *IAM-Policy*.
- Erstellen von stufengerechten Kommunikationsmitteln für die diversen Stakeholder.
- (Optional) Unterstützung bei IAM-Projekten und Spezialvorhaben.
- *IAM-Führung* beraten.

7 IAM-Services

Nachfolgend werden alle *IAM*-Services, welche von den verschiedenen Akteuren (siehe Kapitel 3.1) angeboten werden, beschrieben. Es handelt sich dabei um Schnittstellen für die Prozesse (siehe Kapitel 6) und nicht um technische Service-Komponenten, d. h. bei einer Realisierung können ein oder auch mehrere *IAM-Services* von einer technischen Service-Komponente implementiert oder auch ein *IAM-Service* auf mehrere technischen Service-Komponenten verteilt werden.

Die Modelle dieses Kapitels beschreiben sowohl die *Laufzeit*, wenn ein *Subjekt* versucht auf eine *Ressource* zuzugreifen, als auch die *Definitionszeit*, während der die verschiedenen (Meta)-Daten erfasst und gepflegt werden. Die *IAM-Services* zu den Prozesse *IAM steuern, IAM führen* und *IAM unterstützen* (vgl. Abschnitt 6) sind in diesem Standard nicht dargestellt.

In den Abbildungen werden die *IAM-Services* der *Definitionszeit* (hellblau dargestellt) und die *IAM-Services* der *Laufzeit* (dunkelblau dargestellt) optisch von den Realweltobjekten (grün dargestellt) abgetrennt.

Das *Identitäts- und Berechtigungsmanagement* der hier vorgestellten *IAM-Services* ist nicht Inhalt dieses Standards. Grundsätzlich kann jede Verwendung eines *IAM-Services* nach den Realweltobjekten *Subjekt* und *Ressource* aufgelöst betrachtet werden und der vorliegende Standard rekursiv angewandt werden. Ob dies sinnvoll ist, muss im konkreten Anwendungsfall entschieden werden.

7.1 Realweltobjekte

Die Realweltobjekte und ihre Aufgaben werden nachfolgend genauer beschrieben. Sie sind in allen Modellen immer hellgrün dargestellt.

7.1.1 Subjekt

Subjekt	Eine *natürliche Person*, eine *handelnde Organisation*, ein *Service* oder ein *Ding*, das auf eine *Ressource* zugreift oder zugreifen möchte. Ein *Subjekt* wird durch *E-Identities* repräsentiert.

Aufgaben (zur Laufzeit):

- *Authentisiert* sich.
- (optional, nur für *natürl. Personen*) Gibt die *Authentifizierungsbestätigung* für die *RP* frei.
- (optional, nur für *natürl. Personen*) Gibt den Versand der *Attribute* frei.
- Greift auf *Ressourcen* zu.

7.1.2 Ressource

Ressource	Service oder Daten, auf welche ein *Subjekt* zugreifen kann, wenn es sich *authentisiert* hat und es auf der Basis der benötigten *Attribute* autorisiert wurde.

Aufgaben (zur *Laufzeit*):

- Stellt dem *Subjekt* ihre fachliche Leistung (Funktionalität) zur Verfügung (die dem *Identifikator* entsprechenden Informationen oder Services)

7.2 IAM-Services zur Definitionszeit

In Abbildung 16 sind die *IAM-Services* zur *Definitionszeit* (in den Modellen hellblau), die zur Verwaltung der verschiedenen Informationselemente benötigt werden, dargestellt. Die erste Gruppe bezieht sich auf das Subjekt. Die zweite Gruppe definiert Elemente in Abhängigkeit der *Ressource*.

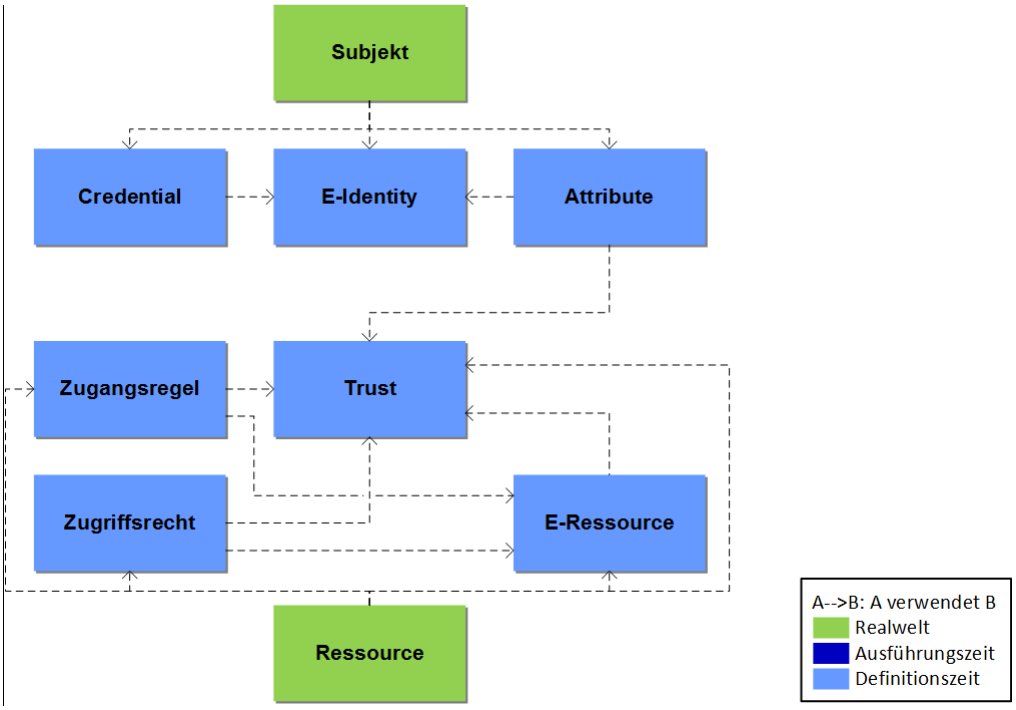


Abbildung 16 IAM-Services – Definitionszeit

7.2.1 E-Identity Service

E-Identity Service	Der *E-Identity Service* stellt zu *Subjekten E-Identities* aus und verwaltet sie.

Prozess: *E-Identity definieren* (6.2.1)

Schnittstellen:

In: *Subjekt*,

(*E-Identities)*

Out: E-Identities

7.2.2 Credential Service

Credential Service	Der *Credential* Service gibt *Authentifizierungsmittel* aus und verwaltet sie. Er ermöglicht eine benutzerfreundliche Erneuerung bzw. den Ersatz von Authentifizierungsmitteln. Ein *Authentifizierungsmittel* bezieht sich auf eine *E-Identity* und ist auf ein bestimmtes *Subjekt* ausgestellt.

Prozess: *Authenitifizierungsmittel definieren* (6.2.3)

Schnittstellen:

In: E-Identity,

Authentifizierungsfaktoren,

(Authentifizierungsmittel)

Out: *Authentifizierungsmittel, Credential*

7.2.3 Attribute Service

Attribute Service	Der *Attribute Service* pflegt zeitnah ein oder mehrere *Attribute* für definierte *Subjekte*.

Prozess: *Attribute definieren* (6.2.2)

Schnittstellen:

In: *E-Identity*, *Eigenschaften* des *Subjektes*

Out: *Attribute*

7.2.4 Trust Service

Trust Service	Der *Trust Service* pflegt die akzeptierten, vertrauenswürdigen *IAM-Dienstanbieter* und *Relying Parties*.

Prozess: *IAM-Führung führen* (6.3.7)

Schnittstellen:

In: Informationen darüber wer wem bezüglich was vertraut,

Metadaten der *RPs* und *IAM-Dienstanbieter*,

Metadaten der *Attribute* der *APs*

Out: Trust,

Metadaten der *RPs* und *IAM-Dienstanbieter*

7.2.5 E-Ressource Service

E-Ressource Service	Der *E-Ressource* Service stellt zu *Ressourcen E-Ressourcen* aus und verwaltet sie.

Prozess: *E-Ressource definieren* (6.2.4)

Schnittstellen:

In: *Ressource* einer *Relying Party*

Out: *E-Ressource und Metadaten*

7.2.6 Zugangsregel Service

Zugangsregel Service	Der *Zugangsregel Service* verwaltet die Regeln für den Zugang zu einer *E-Ressource*. Die Regeln sind auf der Basis von *Authentisierung*, *Attributen,* Kontext des *Zugriffs* (Lokation, Zeitpunkt, *Vertrauensstufe* usw.) oder eigenen Modellen (Gruppen, Rollen, Einzelberechtigungen) definiert.

Prozess: *Zugangsregeln für E-Ressourcen definieren* (6.2.5)

Schnittstellen:

In: Trust-Beziehungen,

E-Ressourcen,

Art und Qualität der *Attribute* (Metadaten der *Attribute*),

Art, Qualität und Kontext der *Authentifizierung*

Out: *Zugangsregeln*

7.2.7 Zugriffsrecht Service

Zugriffsrecht Service	Der *Zugriffsrecht* Service verwaltet die Rechte für die Nutzung einer *E-Ressource*. Die *Rechte* sind auf der Basis von *Authentisierung*, *Attributen,* Kontext des *Zugriffs* (Lokation, Zeitpunkt, *Vertrauensstufe* usw.) oder eigenen Modellen (Gruppen, Rollen, Einzelberechtigungen) definiert.

Prozess: *Zugriffsrechte für E-Ressource definieren* (6.2.6)

Schnittstellen:

In: Trust-Beziehungen,

E-Ressourcen,

Art und Qualität der *Attribute* (Metadaten der *Attribute*),

Art, Qualität und Kontext der *Authentifizierung*

Out: *Zugriffsregeln*

7.3 IAM-Services zur Laufzeit

Die IAM-Services zur *Laufzeit* (in den Modellen dunkelblau) sind in Abbildung 17 dargestellt. Die Abbildung enthält alle *IAM-Services*, die zur Abwicklung des Prozesses *Zugriff kontrollieren* zur *Laufzeit* verwendet werden.

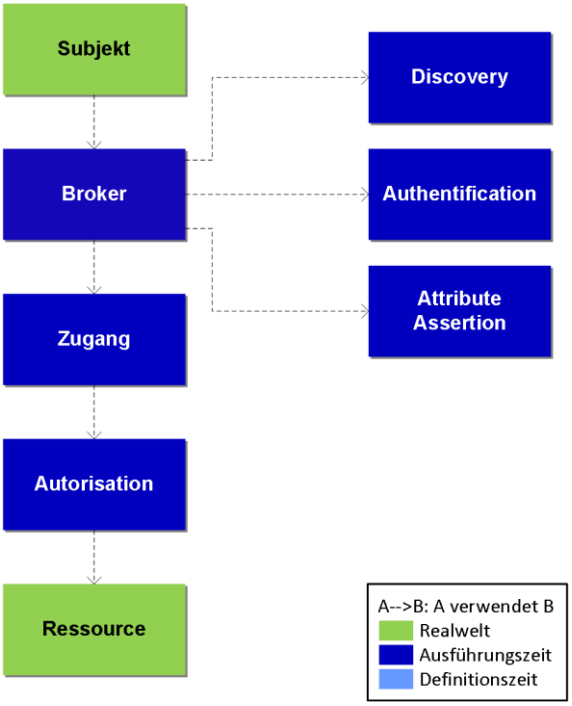


Abbildung 17 IAM-Services – Laufzeit

7.3.1 Discovery Service

Discovery Service	Der *Discovery Service* stellt eine Auswahl von *IdPs* bereit, bei der das *Subjekt* einen *IdP* auswählen kann.

Prozess: *IdP Discovery* (6.1.2)

Schnittstelle:

In: (minimale geforderte *Vertrauensstufe*)

Out: Gewählter *IdP*

7.3.2 Authentication Service

Authentication Service	Der *Authentication* Service überprüft mittels der *Authentifizierungsmittel*, ob der Zugreifende (*Subjekt*) der ist, der er behauptet zu sein.

Prozess: *Subjekt authentifizieren* (6.1.3)

Schnittstelle:[9]

In: *Authentifizierungsanfrage* (*Authentication Request)*,
(*Identifikator)*,
Authentifizierungsfaktoren

Out: *Authentifizierungsbestätigung* (Angabe, ob die Überprüfung des *Subjekts* positiv ausgefallen ist oder nicht),
(*Identifikator*),
Art und Qualität der *Authentifizierung*

Braucht*: Credential Service, Logging Service*

7.3.3 Attribute Assertion Service

Attribute Assertion Service	Der *Attribute Assertion Service* stellt die *Attributbestätigungen* über eine definierte Schnittstelle aus.

Prozess: *E-Identity anreichern* (6.1.4)

Schnittstelle:

In: Attributanfrage (Attribute-Request),
Identifikator,
(Authentifizierungsbestätigung)

Out: *Attributbestätigung* (Angabe, ob die Überprüfung der Beziehung zwischen einem *Attribut* und dem *Subjekt* positiv ausgefallen ist, oder nicht).

Braucht: *Attribute Service, Logging Service*

7.3.4 Broker Service

Broker Service	Dieser *IAM-Service* vermittelt zwischen dem *Subjekt*, *Ressourcen* und den *IAM-Services* der *Laufzeit*, föderiert *Authentifizierungs-* und *Attributbestätigungen*.

Prozess: *E-Identity bestätigen* (6.1.1)

Schnittstelle:

In: (minimale geforderte *Vertrauensstufe*),
(*Identifikator),*
Trust

Out: *Authentifizierungsbestätigungen,*
(Attributbestätigungen)

[9] Bei den Services zur Laufzeit werden in der Schnittstelle, die Daten angeben, die zur Laufzeit als Informationen benötigt werden (In-Schnittstelle) bzw. die nach der Ausführung des Services zur Verfügung stehen (Out-Schnittstelle). Werden zur Ausführung zusätzliche Informationen aus der Definitionszeit oder weitere Services der Laufzeit benötigt, so werden die entspr. Services angegeben (Braucht-Schnittstelle).

Braucht: *Trust Service, Authentication Service, Attribute Assertion Service, Logging Service, E-Identity Service*

7.3.5 Zugang Service

Zugang Service	Der *IAM-Service* überprüft die Einhaltung der *Zugangsregeln* und erlaubt dem *Subjekt* den Zugang, wenn die entsprechenden Regeln erfüllt sind.

Prozess: *Zugang erlauben* (6.1.5)

Schnittstelle:

In: *Identifikator* einer *E-Ressource, Authentifizierungs- und Attributbestätigungen*

Out: false oder true + *Authentifizierungsergebnis, (Authentifizierungs-* und *Attributbestätigunge)*

Braucht: *Zugangsregel Service, Logging Service, Broker Service*

7.3.6 Autorisation Service

Autorisation Service	Der *IAM-Service* überprüft zur *Laufzeit* die Einhaltung der *Rechte* für die Nutzung der *E-Ressource* und erlaubt dem *Subjekt* die Nutzung der *Ressource*, wenn es die entsprechenden *Rechte* besitzt.

Prozess: *Zugriff erlauben und Attribute nutzen* (6.1.6)

Schnittstelle:

In: *Authentifizierungsbestätigungen*,
Attributbestätigungen,
Identifikator einer *E-Ressource*

Out: Security Token (mit allen für den *Zugriff* auf die *Ressource* relevanten Informationen, insb. *Attributbestätigungen*)

Braucht: *Zugriffsregel Service, Logging Service*

7.3.7 Logging Service

Logging Service	Der *IAM-Service* dokumentiert zur *Lauf-* und *Definitionszeit* die Verwendung eines *IAM-Services* und stellt der Support-Organisation die notwendigen Informationen bereit, um Nutzungsprobleme oder Fehler aufzuklären.

Prozess: Ist in jedem Lauf- und Definitionszeitprozess enthalten

Schnittstelle:

In: Nutzungsdaten eines *IAM-Service*

Out: Logs

Braucht: -

7.4 Gesamtmodell

In Abbildung 18 werden alle *IAM-Services* zusammen dargestellt. Man erkennt, dass die Laufzeitservices zur Erfüllung ihrer Funktionalitäten auf die Daten der *IAM-Services* der *Definitionszeit* zugreifen. Auf die Darstellung des Laufzeitservices *Logging Services*, der von allen anderen *IAM-Services* genutzt wird, wurde aus Übersichtlichkeitsgründen verzichtet.

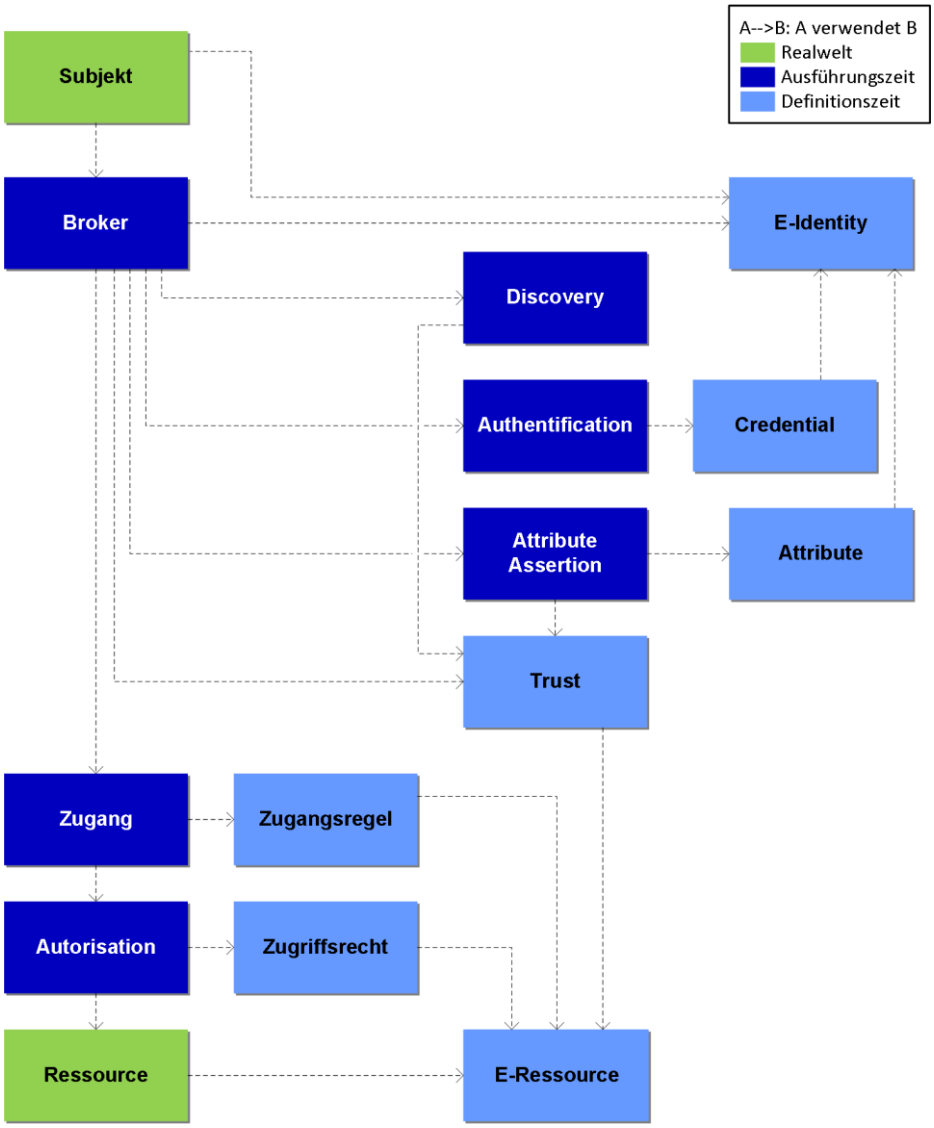


Abbildung 18 IAM-Services – Übersicht

7.5 Prozessunterstützung durch IAM-Services

In diesem Abschnitt wird an den Laufzeitprozessen dargestellt, wie die *IAM-Services* zusammenarbeiten. Die Zusammenarbeit der *IAM-Services* zur Erbringung der Definitionsprozesse ist einfach und in Abbildung 16 und in den *IAM-Services* bereits direkt angesprochen. Diese werden deshalb hier nicht dargestellt.

7.5.1 IdP Discovery

Abbildung 19 zeigt die Verwendungen der *IAM-Services* im Rahmen des Prozesses *IdP Discovery* (6.1.2).

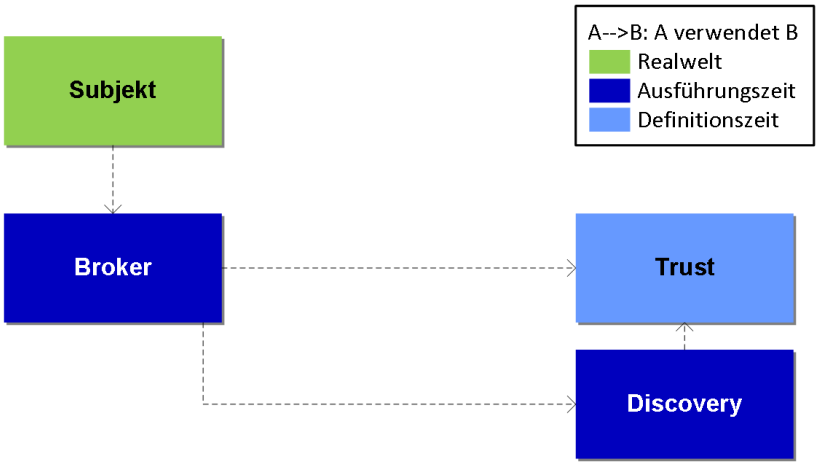


Abbildung 19 Prozessunterstützung *IdP Discovery*

IdP Discovery folgt dem nachstehenden Ablauf:

- Der *Broker Service* prüft, welcher *Authentification Service* und (wenn nötig) *Attribute Assertion* Service gemäss *Trust Service* die Anforderungen des aufrufenden Service erfüllen und stellt eine Auswahl zur Verfügung.
- Das *Subjekt* wählt einen *Authentification Service* (*IdP*) von der Auswahl aus.

7.5.2 Subjekt authentifizieren

Abbildung 20 zeigt die Verwendungen der *IAM-Services* im Rahmen des Prozesses *Subjekt authentifizieren* (6.1.3).

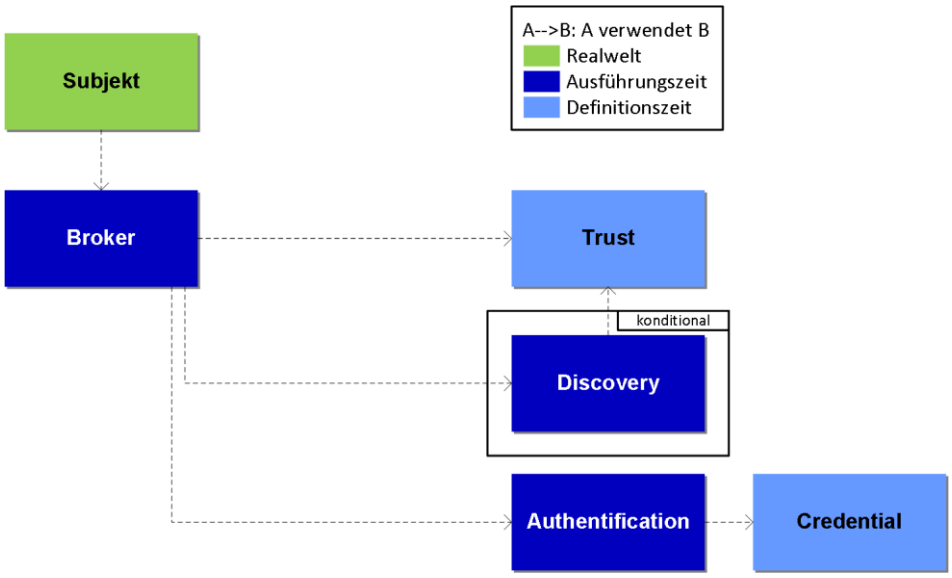


Abbildung 20 Prozessunterstützung *Subjekt authentifizieren*

Subjekt authentifizieren folgt dem nachstehenden Ablauf:

- Der *Broker Service* delegiert die *Authentifizierung* des *Subjekts* an den gewählten *Authentification* Service.
- Das *Subjekt* authentisiert sich gegenüber dem *Authentication* Service. Dieser prüft den generierten Ausgabewert des Authentifikators gegen das *Credential* der behaupteten E-Identity. Ist die Prüfung positiv, ist die Authentifizierung erfolgreich.

7.5.3 E-Identity bestätigen

Abbildung 21 zeigt die Verwendungen der IAM-Services im Rahmen des Prozesses *E-Identity bestätigen*.

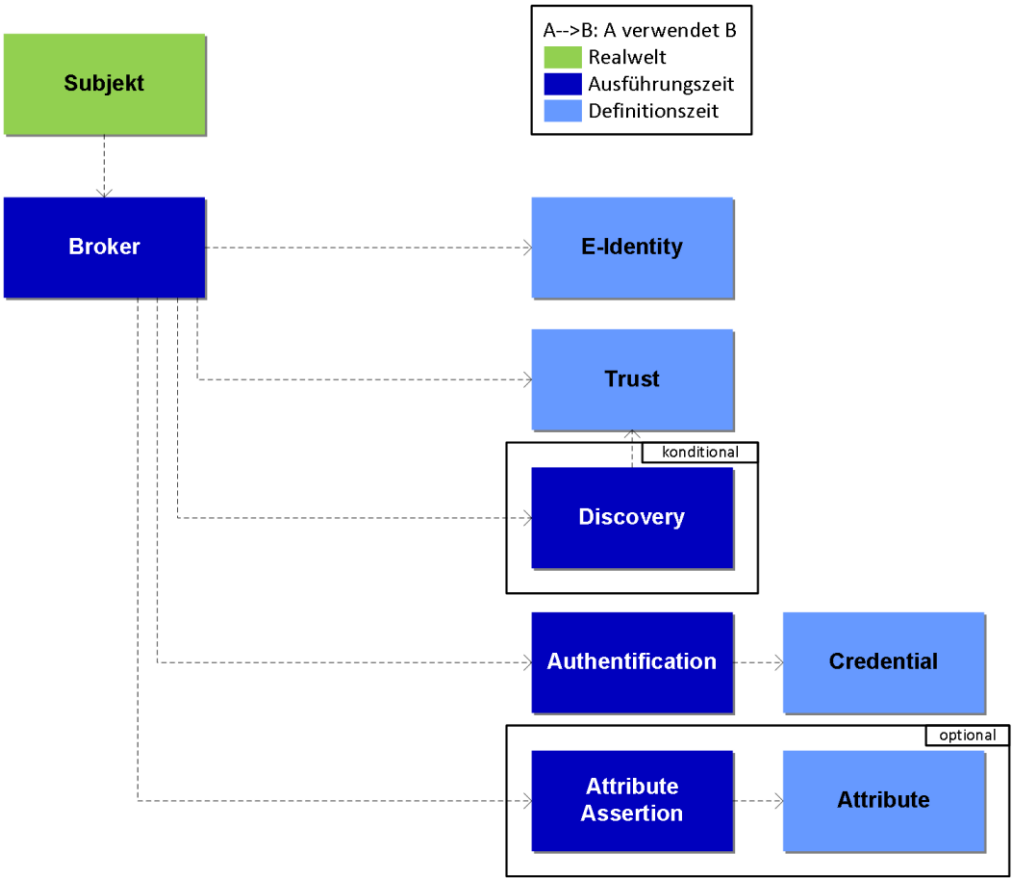


Abbildung 21 Prozessunterstützung *E-Identity bestätigen*

E-Identity bestätigen folgt dem nachstehenden Ablauf:

- Nach erfolgreicher Authentifizierung wird überprüft, ob der aufrufende Service Attribute benötigt.
- (optional) Falls Attribute benötigt werden, wird die *Attribute Assertion* Service-Auswahl auf die reduziert, die gemäss den verlinkten *E-Identities* (linkedID) der *E-Identity* Service Informationen zur *E-Identity* führen.
    - Die E-Identity wird gemäss IAM-Service *E-Identity anreichern (vgl. Abschnitt 7.5.4)* mit Attributen angereichert.
- Der *Broker Service* erzeugt Authentifizierungs- und Attributbestätigung und übergibt diese dem aufrufenden Service

7.5.4 E-Identity anreichern

Abbildung 22 zeigt die Verwendungen der IAM-Services im Rahmen des Prozesses *E-Identity anreichern*.

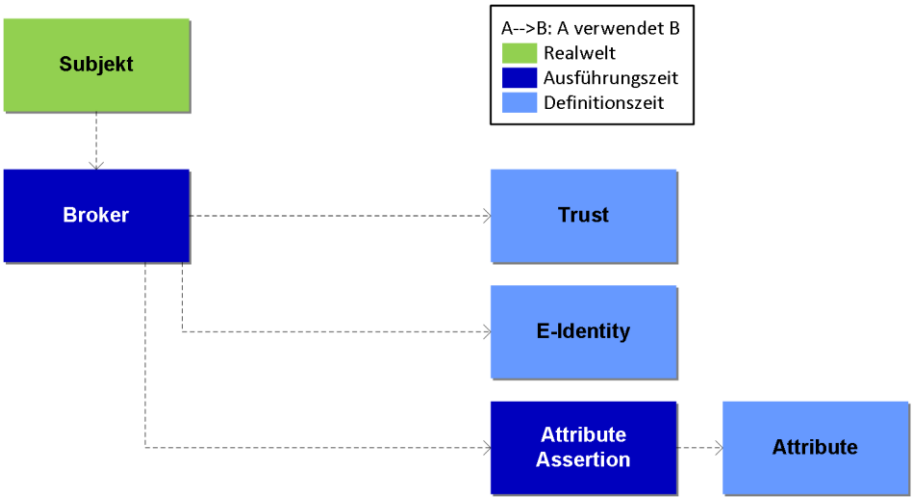


Abbildung 22 Prozessunterstützung *E-Identity anreichern*

E-Identity anreichern folgt dem nachstehenden Ablauf:

- Der *Broker Service* fragt die entsprechenden *Attribute Assertion* Service an, die entsprechenden *Attribute* zu bestätigen.
- (optional) Der *Broker Service* holt die Bestätigung vom Subjekt (nur bei natürlichen Personen) des Ergebnisses der Authentifizierung und die ermittelten Attribute an den aufrufenden Service zu übergeben.

7.5.5 Zugang erlauben

Abbildung 23 zeigt die Verwendungen der IAM-Services im Rahmen des Prozesses *Zugang erlauben.*

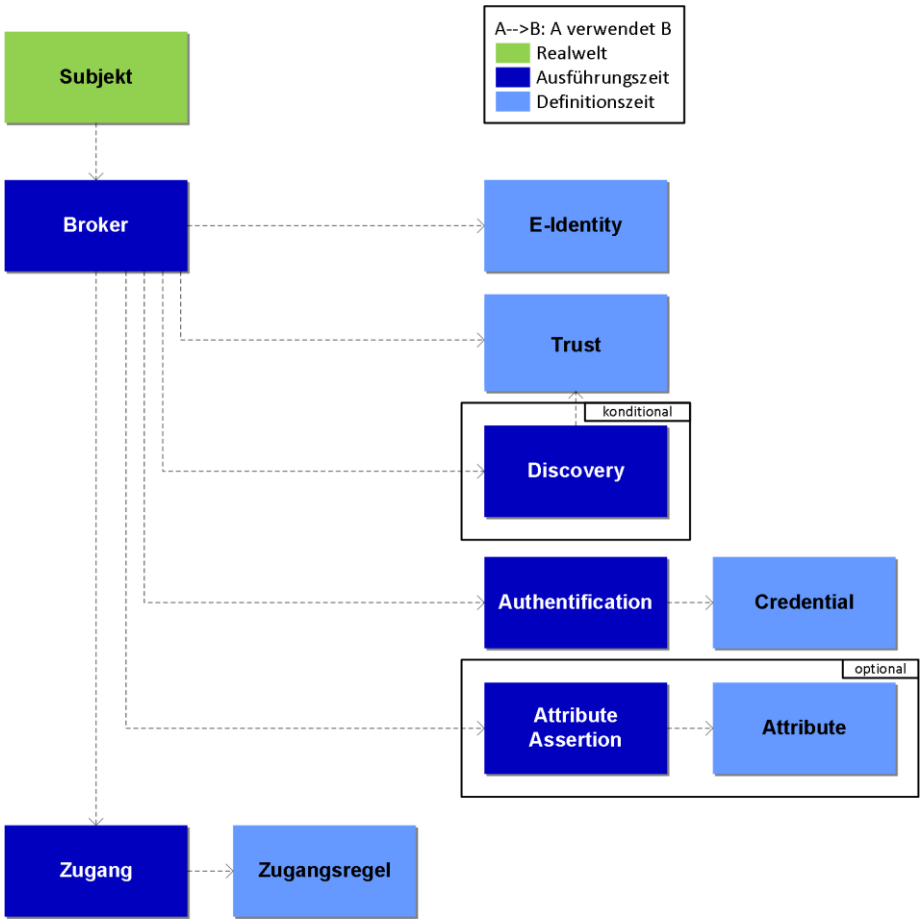


Abbildung 23 Prozessunterstützung *Zugang erlauben*

Zugang erlauben folgt dem nachstehenden Ablauf:

- *Zugang Service* prüft die Zugangsregeln für diese E-Ressource und verlangt vom *Broker Service*, entsprechend den Anforderungen das Subjekt zu authentifizieren und die Attribute zur *E-Identity* zu bestätigen (vgl. Abschnitte 7.5.3 und 7.5.4)
- *Zugang Service* prüft das Zugangsrecht basierend auf den *Authentifizierungs- und Attributbestätigungen.*
- *Zugang* Service gewährt den *Zugang* auf die *Ressource* und übergibt die *Authentifizierungs- und Attributbestätigungen.*

7.5.6 Zugriff erlauben und Attribute nutzen

Abbildung 24 zeigt die Verwendungen der *IAM-Services* im Rahmen des Prozesses *Zugriff erlauben und Attribute nutzen* (6.1.6).

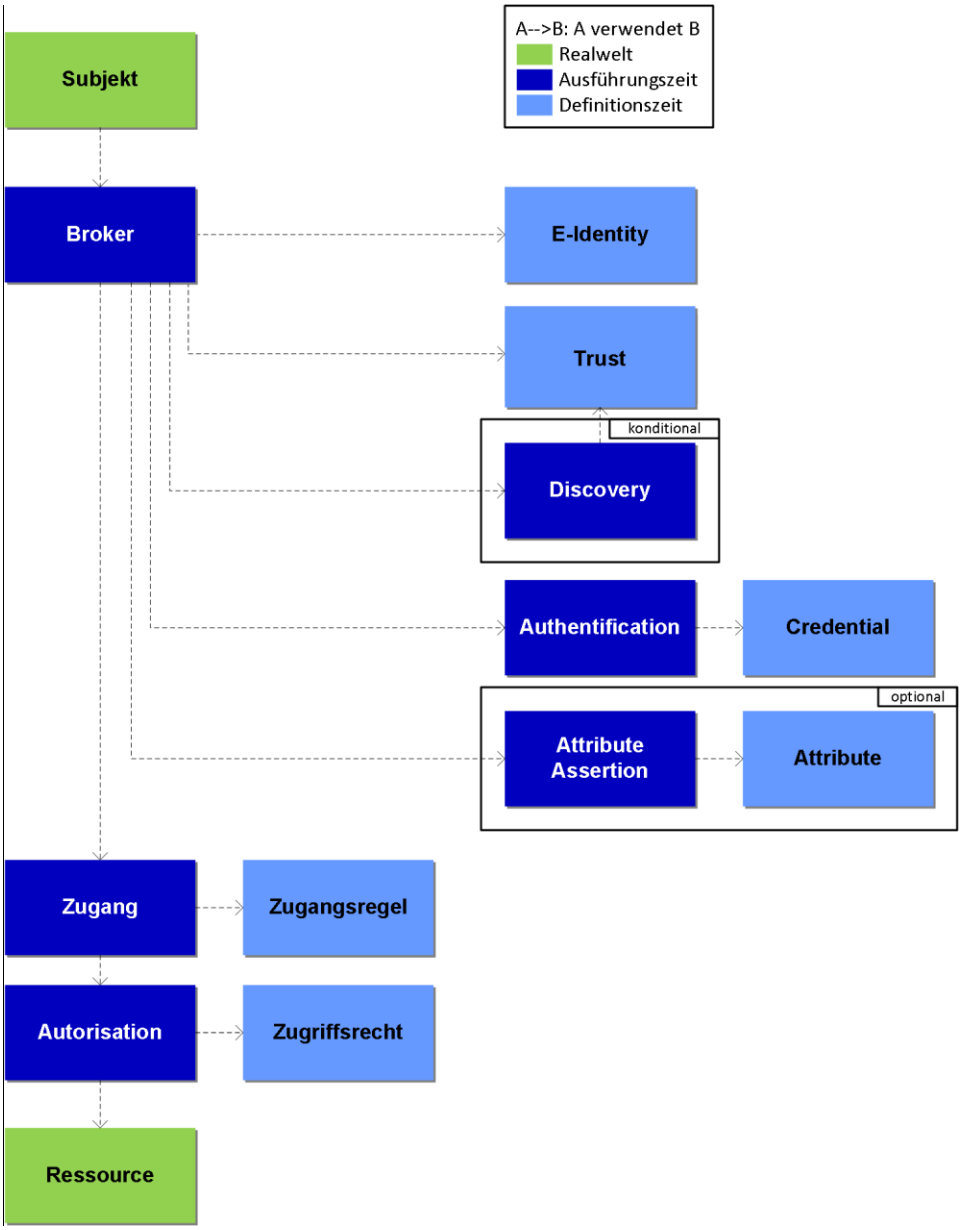


Abbildung 24 Prozessunterstützung *Zugang erlauben und Attribute nutzen*

Zugriff erlauben und Attribute nutzen folgt dem nachstehenden Ablauf:

- *Autorisation* Service prüft die *Zugriffsrechte* für diese *E-Ressource* und verlangt vom *Zugangs Service*, entsprechende *Authentifizierungs-* bzw. *Attributbestätigungen*.
- *Autorisation Service* prüft das *Zugriffsrecht* basierend auf den *Authentifizierungs- und Attributbestätigungen,* Kontext des *Zugriffs* oder eigenen Modellen (Gruppen, Rollen, Einzelberechtigungen).

- *Autorisation* Service gewährt den *Zugriff* auf die *Ressource* und übergibt die *Authentifizierungs-* und *Attributbestätigungen.* Die *Attribute* können nun entsprechend genutzt werden.

7.6 Zuordnung Service zu Informationselemente

Nachfolgende Tabelle stellt die Beziehung zwischen den *IAM-Services* und den Elementen der Informationsarchitektur (Semantik und Schnittstelle) dar. *IAM-Services* in der *Definitionszeit* bearbeiten (B) Objekte und deren Beziehungen zueinander. *IAM-Services* der *Laufzeit* lesen (L) Objekte und deren Beziehungen zueinander. Einzelne *IAM-Services* verwenden allerdings nur die *Metadaten* (M) anderer *IAM-Services*.

		Informationselement										
		E-Identity[10]	**Attribut**[11]	**Zugangsregel**	**Zugriffsrecht**	**E-Ressource**	**Credential**	**Identifikator einer E-Identity**	**Ausgabewert des Authentikator**	**Authentifizierungs-bestätigung**	**Attributbestätigung**	**Identifikator einer E-Ressource**
IAM-Services	E-Identity	B	B[12]					B				
	Credential	L					B	L				
	Attribute	L	B					L				
	Trust	M	M			M						
	E-Ressource					B						B
	Zugangsregel	M	M	B		L						
	Zugriffsrecht	M	M	L	B	L						
	Authentication	L					L	L	B			
	Attribut Assertion		L					L		L	B	
	Broker	L						L	L	LB[13]	LB[13]	
	Zugang			L		L		L		L	L	L
	Autorisation				L	L		L		L	L	L

B = Bearbeiten (Create/Read/Update/Delete), L = Lesen (Read), M = liest nur Metadaten

Tabelle 5 Beziehung zwischen IAM-Services und Semantik des Informationsmodells

[10] inkl. Beziehung *linkedID*
[11] inkl. Beziehung zu *E-Identity*
[12] B für *Identifikator* (ist auch ein *Attribut*)
[13] B, wenn Broker Service selber kombinierte *Authentifizierungs-* und *Attributbestätigungen* ausstellt

7.7 Zuständigkeiten für IAM-Services

Tabelle 6 zeigt auf, welcher Stakeholder idealtypisch welchen *IAM-Service* zur *Definitions-* und *Laufzeit* anbietet. Die *IAM-Services* sind in Kapitel 7 näher beschrieben. Die hier vorgeschlagene Aufteilung optimiert bezüglich Wiederverwendung der *IAM-Services* in einer *Identity Federation*. Die *Relying Party* gibt deshalb möglichst viel Betriebsverantwortung an *IAM-Dienstanbieter*.

		Stakeholder					
		IAM-Dienstanbieter					Relying Party
		IdP	AP	CSP	RA	Vermittler	
IAM-Service	E-Identity				**X**		
	Credential			**X**			
	Attribute		**X**				
	Trust					**X**	
	E-Ressource						**X**
	Zugangsregel					**X**	
	Zugriffsrecht						**X**
	Authentication	**X**					
	Attribute Assertion		**X**				
	Broker					**X**	
	Zugang					**X**	
	Autorisation						**X**

Tabelle 6 Beziehung zwischen IAM-Services und Stakeholder

8 IAM für das IoT

Ein *Ding* im vorliegenden Kontext ist ein physischer Gegenstand, der aktiv und autonom über ein *Netzwerk* mit *Ressourcen* kommuniziert[14]. Mehrere *Dinge*, die im selben *Netzwerk* verknüpft sind, bilden ein Internet der Dinge (*Internet of Things*, IoT). Beispiele sind Roboter, aktive Elemente der Gebäudeautomation, moderne (zukünftig auch selbstfahrende) Autos oder generell Sensorknoten unterschiedlichster Art.

Das Konzept des IoT stammt aus den achtziger Jahren. Autonom agierende *Dinge* gibt es schon seit längerem (z. B. Alarmierungssysteme), die grosse praktische Relevanz des IoT wird sich aber erst im Zuge der weiteren Miniaturisierung und Automatisierung von Fabrikations-, Transport- und Steuerungssystemen erweisen.

Die langfristigen Auswirkungen des IoT auf die Gestaltungsprinzipien der *Identitäts- und Zugriffsverwaltung (IAM)* sind noch nicht absehbar. Dieses Kapitel zeigt auf, in welchen Bereichen solche Auswirkungen zu erwarten sind.

Grundsätzlich ist der Regulator dafür verantwortlich, wie *Dinge* in einem *föderierten IAM-System* verwaltet werden. Dies schliesst das Life-Cycle Management und das Sicherheitskonzept der *Dinge* ein.

Die *Dinge* werden in diesem Standard als *Subjekte* betrachtet. Falls die *Dinge* als *Ressource* betrachtet werden, gibt es keine Besonderheiten gegenüber einer üblichen *Ressource*.

8.1 Spezielle Eigenschaften von Dingen

Dinge (bzw. Things) sind Realweltobjekte, die auf *Ressourcen* zugreifen. In der Informationsarchitektur des vorliegenden Standards sind sie als *Subjekte* mit einer spezifischen *Eigenschaft* abgebildet. Sie unterscheiden sich insbesondere in den folgenden Punkten von *natürlichen Personen*:

- *Dinge* können zu einer *natürlichen Person* oder zu einer *Organisation* gehören, nachfolgend als Besitzer (des *Dings*) bezeichnet. Der Besitzer ist für seine *Dinge* verantwortlich und haftet für deren Aktivitäten im IoT[15].
- Neben dem „Besitz“ können für die Identitäts- und Zugriffsverwaltung von Dingen auch andere Relationen zwischen *Dingen* und *Subjekten* wichtig werden (z. B. „hergestellt von“ oder „benutzt durch“).
- *Dinge* können nur Daten benützen, die in elektronischer Form verfügbar sind. Alle zur *Laufzeit* relevanten Daten wie *Authentifizierungsfaktoren* (z. B. PIN) und Entscheide (z. B. Freigabe von *Attributen*) müssen deshalb zur *Definitionszeit* konfiguriert werden.

[14] In der Literatur wird manchmal *Ding* als Objekt (eng. Object) bezeichnet. Da der Begriff «Objekt» vorbelastet ist (Verwendung in anderen Gebieten), wird die Bezeichnung *Ding* bevorzugt. Die Bezeichnung des Identifikators eines *Dings* ist oft «oid».

[15] Eventuell ist auch der Hersteller des Dings haftbar. Dies wird aber hier nicht weiter vertieft.

- *Dinge* sind häufig aus anderen *Dingen* zusammengesetzt wie beispielsweise ein Gebäude, das Lifte enthält, die wiederum ein Alarmierungssystem enthalten. Oder ein Fahrzeug mit Bordcomputer inklusive Navigationsgerät und Fahrtenschreiber.
- Die Lebensdauer von *Dingen* kann sehr unterschiedlich sein und von wenigen Stunden (evtl. Minuten) bis zu vielen Jahren reichen.
- Die Anzahl der *Dinge* ist langfristig nicht limitiert. Schätzungen gehen von 1‘000 bis 5‘000 Dingen pro Mensch aus. Die skalierbare Verwaltung dieser *Dinge* erfordert einen hohen Automatisierungsgrad.

8.2 Auswirkung auf die IAM Informationsarchitektur

Grundsätzlich sind die *IAM-Services* auch auf *Dinge* anwendbar.

Aufgrund der speziellen Eigenschaften der *Dinge* ergeben sich aber verschiedene Aspekte, die bei der Implementierung betrachtet werden sollten. Viele dieser Aspekte betreffen die IAM Informationsarchitektur und speziell die Verwaltung von komplexen Beziehungen zwischen den *Subjekten*:

Aspekt	Grundsatz, Beschreibung und Umsetzung im IAM
Besitzer[16]	*Dinge* im IoT sollten immer einen Besitzer haben. Der Besitz kann befristet sein (z. B. Miete von Autos oder Ferienwohnungen) oder dauerhaft bis auf Widerruf (der Normalfall). Es kann auch *Dinge* mit mehreren Besitzern geben (z. B. ein Kühlschrank, der Lebensmittel für alle Bewohner einer Wohngemeinschaft nachbestellt). Das Konzept des „Besitzers“ (von *Dingen*) erfordert eine zusätzliche Beziehung im Rahmen der Informationsarchitektur (vergleiche hierzu die Definition *Subjekt* in der Informationsarchitektur). *Bemerkung*: Diese zusätzliche Beziehung kann ggf. auch unabhängig vom IoT genutzt werden, um Abhängigkeiten zwischen *Subjekten* zu verwalten (z. B. Verwaltung von separaten *E-Identities* für IT-Administrator Tätigkeiten).
„On behalf“ Zugriff	*Dinge* nutzen *Ressourcen* „on behalf“ ihres Besitzers. Das Auto sucht sich einen freien Parkplatz oder eine Tankstelle, das Mobiltelefon aktualisiert lokale Daten, der Kühlschrank bestellt Milch. Dies erfordert die Möglichkeit, dass eine *natürliche Person* oder eine *Organisation Attribute* ihrer *E-Identity* temporär oder dauerhaft auf die *E-Identities* ihrer *Dinge* übertragen kann.

[16] Da IoT eine relativ neues Informatik-Thema ist, wird auf die juristische Trennung zwischen Eigentümer und Besitzer nicht eingegangen.

Eigene und übertragene Attribute	*Dinge* haben eigene und übertragene *Attribute*. Eigene *Attribute* sind statisch inhärent (z. B. Seriennummer, Produktionsdatum) oder dynamisch (z. B. aktueller Standort, aktueller Energieverbrauch, derzeit aktiver Authentisierungsschlüssel). Übertragene *Attribute* stammen vom Besitzer wie beispielsweise dessen Organisationszugehörigkeit, Postadresse oder Bankverbindung. Für die Übertragung von *Attributen* an *Dinge* müssen Regeln definiert werden. Beispiele für solche Übertragungsregeln könnten sein: • *Attribute* können nur von *natürlichen Personen* übertragen werden (bei *Organisationen*: Durch einen hierzu autorisierten Vertreter). • Es ist ersichtlich, dass ein *Attribut* übertragen wurde und von wem. • Übertragene *Attribute* werden entzogen, sobald sie dem Übertragenden entzogen werden. • Bei der Übertragung eines *Attributs* wird definiert, ob die Übertragung auch transitiv wirkt (insb. Bei zusammengesetzten *Dingen* relevant). (Bsp. Ein Navigationsgerät eines Fahrzeugs. Kann dieser das Attribut «Automodell» mitteilen?)
Besitzer Wechsel	*Dinge* können den Besitzer wechseln. Langlebige *Dinge* (z. B. Investitionsgüter) können im Verlauf ihrer Lebensdauer mehrfach den Besitzer wechseln. Eigene (inhärente und dynamische) *Attribute* bleiben beim Besitzerwechsel unverändert. Übertragene *Attribute* müssen gelöscht und vom neuen Besitzer ggf. erneut übertragen werden. Ausserdem ist sicherzustellen, dass zu jedem Zeitpunkt ein Besitzer definiert ist.
Ersatz von Dingen	*Dinge* können ersetzt werden. Kurzlebige Dinge (z. B. Verbrauchsmaterial) können 1:1 ersetzt werden. Eigene (inhärente und dynamische) *Attribute* werden beim Ersatz neu definiert. Übertragene *Attribute* müssen automatisch auf das Ersatz-*Ding* übertragen werden können.
Zusammengesetzte Dinge	*Dinge* können aus *Dingen* zusammengesetzt sein. Komplexe *Dinge* sind aus *Dingen* zusammengesetzt, wobei keine Beschränkung in der Verschachtelungstiefe besteht. Ein *Ding* kann sogar zu mehreren übergeordneten *Dingen* gehören wie beispielsweise ein intelligenter Stromzähler, der sowohl zu einem Gebäude als auch zum regionalen Verbund des Netzbetreibers gehört. Das *IAM* muss in der Lage sein, auch komplexe Beziehungen von *Dingen* untereinander abzubilden, so dass auch das Hinzufügen und Entfernen von Dingen möglich ist.

8.3 Auswirkung auf die IAM-Services

Die speziellen Eigenschaften von *Dingen* wirken sich auch auf *IAM-Services* aus:

Aspekt	Grundsatz, Beschreibung und Umsetzung im IAM
Integriertes Authentifizierungsmittel	*Dinge* können ein integriertes *Authentifizierungsmittel* aufweisen. Damit ein *Ding* autonom und ohne manuelle Interaktion einer *natürlichen Person* aktiv werden kann, müssen alle für die *Authentifizierung* zur *Laufzeit* erforderlichen Daten in elektronischer Form verfügbar sein. Dies betrifft insbesondere kryptographische Schlüssel mit den dazugehörigen Aktivierungsdaten (z. B. PIN). Der *Authentication Service* zur *Authentifizierung* von *Subjekten* muss die spezifischen *Eigenschaften* von *Dingen* berücksichtigen.
Automatische Registrierung inkl. Inventarisierung	*Dinge* können sich automatisch registrieren. Damit die langfristig zu erwartende sehr grosse Anzahl von *Dingen* verwaltet werden kann, sind weitgehend automatisierte Verwaltungsprozesse erforderlich. Dies betrifft insbesondere die Registrierung und Inventarisierung von *Dingen*, wenn sie ins Internet der Dinge neu aufgenommen (oder später wieder aus diesem entfernt) werden. Der *E-Identity Service* und der *Credential Service* müssen die spezifischen *Eigenschaften* von *Dingen* berücksichtigen und insbesondere Automatisierung ermöglichen.

9 Privacy

Dieses Kapitel beschreibt Anforderungen zum Schutz der Privatsphäre des *Subjektes*, die über die subjektbezogenen Anforderungen in Kapitel 4.3.1 hinausgehen. Der Schutz der Privatsphäre ist entscheidend für das Vertrauen in das IAM-System, besonders bei Szenarien, bei denen die Einwohnerschaft auf staatliche oder behördliche *Ressourcen* zugreifen (C2G-Szenarien).

Für die Definition und Einhaltung der spezifischen Anforderungen zum Schutz der Privatsphäre ist der *Regulator* verantwortlich. Er sollte über die getroffenen Massnahmen mit allen Beteiligten entsprechend transparent kommunizieren.

9.1 Anforderungen an Sicherheit und zum Schutz der Privatsphäre

In diesem Kapitel werden die allgemeinen Anforderungen an Sicherheit und zum Schutz der Personendaten eines *Subjektes* in einem *föderierten IAM-System* aufgelistet. Je nach Rahmenbedingungen und gewähltem *Identity Federation* Modell sollten die gewünschten Anforderungen bei der Umsetzung mitberücksichtigt werden. Das gilt besonders für Modelle mit zentralem *Vermittler*.

ID	Definition	Anforderung	Anwendung in föderiertem IAM
R1	**Nichtverfolgbarkeit (Untraceability)**	Ein *Subjekt* kann auf eine *Ressource* oder auf einen Dienst zugreifen, ohne dass andere Teilnehmer im System dies feststellen können.	Ein an einem Authentisierungsvorgang beteiligtes System soll ohne Drittpartei nicht feststellen können, ob und wann ein *Subjekt* eine *Ressource* oder einen anderen Dienst benutzt hat.
R2	**Nichtbeobachtbarkeit (Unobservability)**	Ein *Subjekt* kann auf eine *Ressource* oder auf einen Dienst zugreifen, ohne dass unberechtigte Dritte dies feststellen können.	Ein in einem Authentisierungsvorgang unbeteiligtes System soll nicht feststellen können (z.B. durch Überwachung der Kommunikationsvorgänge oder zeitliche Korrelation), ob und wann ein bestimmtes *Subjekt* einen Dienst benutzt hat.
R3	**Unverkettbarkeit (Unlinkability)**	Ein Benutzer kann mehrmals auf eine *Ressource* zugreifen, ohne dass Teilnehmer im System oder unberechtigte Dritte diese Ereignisse verbinden können.	Ein *Subjekt* soll wiederholt auf unterschiedliche *RPs* zugreifen können, ohne dass dessen Identität durch die beteiligten Systeme oder durch Dritte aufgedeckt werden kann (z.B. durch Korrelation der übermittelten *Identifikatoren*).

ID	Definition	Anforderung	Anwendung in föderiertem IAM
R4	**Vertraulichkeit (Confidentiality)**	Personenidentifizierende oder sensitive Informationen dürfen nur von berechtigten Systemen und vom *Subjekt* selbst eingesehen werden können.	Ein an einem Authentisierungsvorgang beteiligtes, nicht vertrauenswürdiges System darf Identitätsinformationen (vermittelte *Attribute*) nicht einsehen und/oder die Identität des *Subjekts* nicht feststellen können. (z.B. durch ‚*end-to-end*' Verschlüsselung).
R5	**Datenherkunft und -unversehrtheit (Authenticity & Integrity)**	Eine *RP* kann die Herkunft, Echtheit und Unversehrtheit von Identitätsinformationen eines *Subjekts* bis zu ihrer Quelle zurück überprüfen.	Eine *RP* kann feststellen, ob eine *Authentifizierungs-* und *Attributbestätigung* von der erwarteten und ihr bekannten autoritativen Quelle stammt.
R6	**Einwilligung/Weitergabe (Consent)**	Die Weitergabe von Identitätsinformationen an einen anfragenden Dienst kann ohne Einwilligung des *Subjekts* nicht erfolgen.	Die Einwilligung zur Weitergabe von personenidentifizierenden Informationen wird vom einem dafür zuständigen System (*Vermittler*, *IdP* oder *AP*) beim *Subjekt* eingeholt. Die Einwilligung umfasst auch den Verwendungszweck der Daten.
R7	**Auskunftsrecht (Right to Information)**	Eine datenbearbeitende Stelle muss jederzeit einem *Subjekt* über die von ihr bearbeiteten Daten des *Subjekts* Auskunft geben können.	Die an einem Authentisierungsvorgang beteiligten Systeme müssen über die Daten, die über ein *Subjekt* erfasst, bearbeitet, verknüpft, gespeichert und weitergegeben wurden jederzeit Auskunft geben können.
R8	**Abfrageberechtigung (Request Permission)**	Es dürfen nur Informationen zu einem *Subjekt* von dazu berechtigten Systemen bearbeitet werden.	Eine RP darf nur Informationen über ein *Subjekt* abfragen können, zu welchen sie berechtigt ist.
R9	**Nachvollziehbarkeit (Auditability)**	Die zu einem bestimmten Authentisierungsvorgang vermittelten Informationen und ihre *Metadaten* müssen vorliegen.	Die vermittelten Identitätsinformationen und ihre *Metadaten* können zentral eingesehen oder unter Mitwirkung aller beteiligten Entitäten im Nachhinein zusammengestellt werden.

Tabelle 7: Anforderungen zum Schutz der Privatsphäre

9.2 Verwaltung und Verarbeitung von Daten von Subjekten

Dieses Kapitel gibt eine Richtlinie, was es zu beachten gibt, wenn Daten von *Subjekten* verwaltet und verarbeitet werden. Die wichtigste Voraussetzung ist, dass der Benutzer jederzeit sicherstellen kann, auf welche Art seine Daten verwendet werden. Dieses Kapitel beschreibt, bei welchen Szenarien welche Massnahmen für den Datenschutz zu beachten sind. Dies soll die Vertrauenswürdigkeit der *Dienstanbieter* stärken.

Minimierung der Datensammlung und des Datenbestands

Subjektidentifizierende *Attribute* dürfen von der *RA* für die Identifizierung und Überprüfung eines Subjektes gesammelt werden.
Ein *Vermittler* darf nur die *Attribute* an eine *RP* weitergeben, welche von der *RP* explizit angefordert wurden. In spezifischen Fällen ist es nicht nötig, *Attribute* völlig offen zu legen. Beispielsweise wenn die *RP* nur wissen will, ob das *Subjekt* 18 Jahre oder älter ist, sollte nicht das explizite Geburtsdatum weitergegeben werden.
Ausserdem darf eine *RP* nur die *Attribute* vom *Subjekt* anfragen, die sie für die Erfüllung ihrer Funktion benötigt. Das Anfragen unnötiger Attribute kann das Vertrauen schwächen.

Verhindern von Profiling

Das Verknüpfen von Daten, die auf ein *Subjekt* zurückführen können, sollte auf ein Minimum reduziert werden. Das Erstellen von Persönlichkeitsprofilen sollte durch organisatorische und technische Massnahmen verhindert werden.
Der Regulator definiert die organisatorischen und technischen Massnahmen für das IAM-System und sollte diese an die weiteren Akteure publizieren.

Kenntnisnahme und Einwilligung

Das *Subjekt* muss immer informiert werden, welche *Attribute* in welcher Form verwendet werden. Die Weitergabe von *Attributen* (z.B. bei Föderierung) ist nur zulässig, nachdem das *Subjekt* mindestens beim ersten Mal explizit zugestimmt hat.

Nutzungsbeschränkung

Ein *Dienstanbieter* muss zu jederzeit transparent Auskunft geben können, welche Daten aus welchem Grund angefragt und bearbeitet werden[17]. Subjektidentifizierende Daten dürfen nicht ohne Einverständnis des *Subjekts* an Dritte weitergegeben werden, ausser es ist gesetzlich anders geregelt.

Datenschutz- und Risikoanalyse

Datenschutz- und Risikoanalysen sollen helfen, den Schutzbedarf einer *Ressource* einzuschätzen und entsprechende Massnahmen zu konzipieren, um den Schutz der Daten nach gesetzlichen Bestimmungen und gängiger Praxis zu gewährleisten.

Datenschutzmassnahmen

Ausgearbeitete Datenschutzmassnahmen sollen die Vertrauenswürdigkeit der *Dienstanbieter* wahren. Die Datenschutzmassnahmen sollen entsprechend des Schutzbedarfes der Daten und an die im Umfeld etablierten Prozesse angepasst sein.

[17] Der Regulator bestimmt wie die Auskunftspflicht wahrgenommen wird. Die Benutzer haben auch das Recht zu erfahren, wie die persönlichen Daten verwendet werden und können dies anfragen, bevor die Daten erhoben werden.

10 Identity Federation Modelle

Die Topologie eines *Identity Federation* Systems beschreibt die Anordnung der verschiedenen Komponenten und ihre logischen Verbindungen. Je nach Rahmenbedingungen und Anforderungen können vier grundlegende Anordnungen unterschieden werden, die in den folgenden Kapiteln kurz beschrieben werden.

10.1 RP-zentriertes Modell

Das *RP-zentrierte Modell* ist in Abbildung 25 dargestellt. Der Vorteil für eine *Relying Party (RP)* liegt darin, dass sie *E-Identities* nicht selbst verwalten muss, sondern die Authentifizierung des Subjekts an eine der vertrauenswürdigen IdPs delegieren kann.

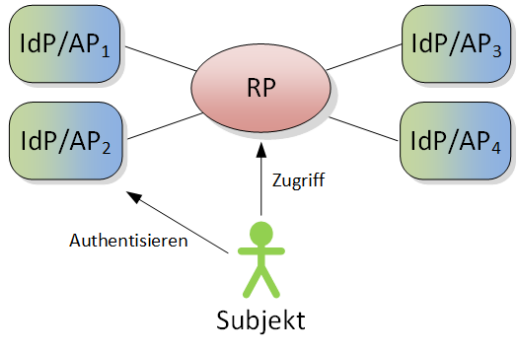


Abbildung 25 RP-zentriertes Modell

10.2 IdP-zentriertes Modell

Ein anderes typisches Szenario ist das *IdP-zentrierte Modell* (vgl. Abbildung 26). In diesem Modell authentisiert sich ein *Subjekt* bei einem zentralen *IdP/AP* (z.B. seiner Heim-Organisation), um die Authentifizierungsbestätigung für den transparenten *Zugriff* auf verschiedene *RPs* zu verwenden.

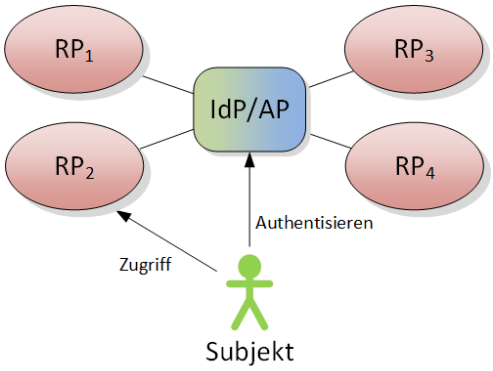


Abbildung 26 IdP-zentriertes Modell

10.3 Full-meshed Modell

Wie in Abbildung 27 dargestellt, föderieren in einem *full-meshed* Modell mehrere Organisationen gegenseitig Identitäten über ihre Organisationsgrenzen hinweg. Jede Organisation

tauscht in einem *full-meshed* Modell alle notwendigen Informationen der eigenen Systeme mit den Partnerorganisationen aus.

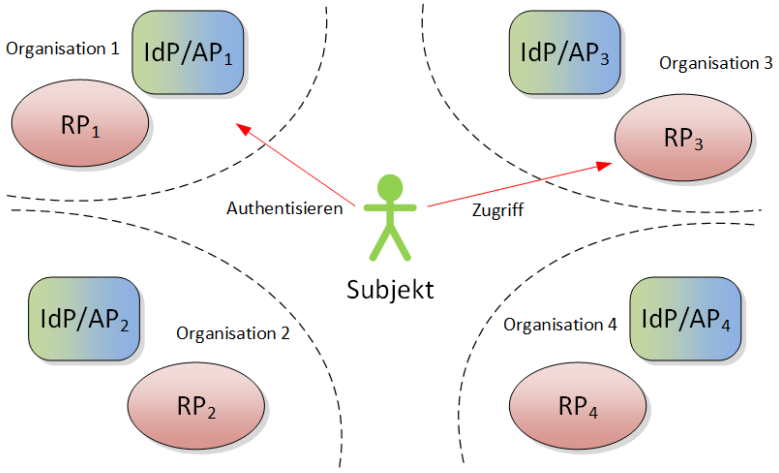


Abbildung 27: Full-meshed Modell

10.4 Hub-'n'-Spoke Modell

Ein Hub-'n'-Spoke[18] Modell basiert auf einer zentralen Vermittlerinfrastruktur - dem *Broker*. Alle beteiligten Parteien vertrauen diesem *Vermittler*. Wie in Abbildung 28 gezeigt, kommunizieren Identitätslieferanten (*IdP/AP*) und -konsumenten (*RP*) nicht mehr direkt miteinander. Sie tauschen ihre Nachrichten über den *Broker* aus, welcher diese prüft und an den richtigen Empfänger weiterleitet.

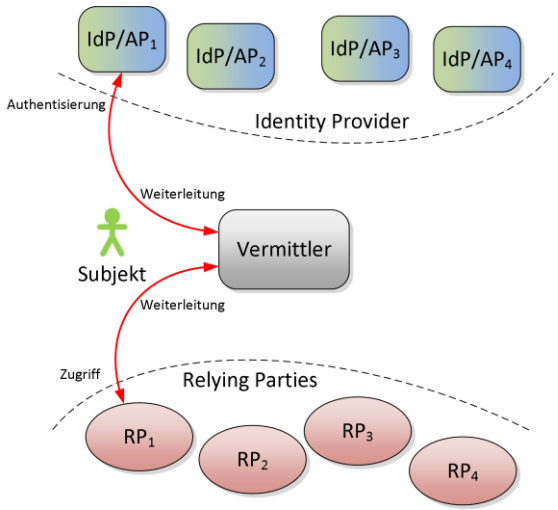


Abbildung 28: Hub-'n'-Spoke Modell

[18] Nabe und Speiche

11 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellt, oder welche **eCH** referenziert, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen, ist, soweit gesetzlich zulässig, wegbedungen.

12 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen & Bibliographie

[1] A. Laube-rosenpflanzer, A. Spichiger, T. Kessler, A. Müller, and M. Kunz, “eCH-0219 - IAM-Glossar,” vol. 1.0, 2017.

[2] W. Müller and H. Lindner, “eCH-0122 – Architektur E-Government Schweiz : Grundlagen Dokument,” vol. 1.0, pp. 1–26, 2014 [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0122

[3] Wikipedia, “IT Infrastructure Library.” [Online]. Available: https://de.wikipedia.org/wiki/IT_Infrastructure_Library

[4] “Protokoll Expertenworkshop ‘Sicherheitsopportunitäten für den Wirtschaftsstandort Schweiz’ vom 8.11.2012 (zu Strategie Informationsgesellschaft),” 2012.

[5] M. Topfel, T. Jarchow, A. Spichiger, and R. Bernold, “eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID,” vol. 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=a26d17d1-fe03-4226-97ab-9beefef22856

[6] International Standards Organisation, “ISO 31000 - Risk management,” *ISO 31000:2009 - Risk Management*. p. 1, 2009 [Online]. Available: http://www.iso.org/iso/home/standards/iso31000.htm

[7] ISACA, *COBIT 5 Framework*. 2012 [Online]. Available: www.isaca.org/COBIT

[8] P. Editors, W. Fumy, M. De Soete, E. J. Humphreys, K. Naemura, and K. Rannenberg, “ITU-T Recommendation X . 1254 | International Standard ISO / IEC DIS 29115 Information technology — Security techniques — Entity authentication assurance framework,” 2011.

[9] Europäische Union, “Durchführungsverordnung (EU) Nr. 2015/1502 der Kommission vom 8. September 2015,” no. September, 2012.

[10] H. Häni and U. Kienholz, “eCH-0172 IAM-Maturitätsmodell,” vol. 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=a26d17d1-fe03-4226-97ab-9beefef22856

[11] A. Laube-Rosenpflanzer, G. Hassenstein, M. Kunz, T. Gruoner, A. Spichiger, and T. Selzam, “eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten,” vol. 2.0, 2017 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=54cce841-215f-4887-9382-25620dcbf9b1

[12] ISO/IEC, “ISO/IEC 27001:2013” [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[13] A. Laube-rosenpflanzer, G. Hassenstein, S. Agosti, M. Vinzens, U. Pfenninger, and D. Leiser, “eCH-0168 SuisseTrustIAM technische Architektur und Prozesse,” vol. 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=31499686-813d-4589-b794-11015fbf2059

[14] A. Laube-rosenpflanzer and G. Hassenstein, “eCH-0174 SuisseTrustIAM - Implementierung mit SAML 2.0,” vol. 1.0, 2015 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=5d8ee101-aba3-4061-aba0-aaed23b1f04f

Anhang B – Mitarbeit & Überprüfung

Gruoner Torsten	ISB
Hassenstein Gerhard	Berner Fachhochschule, TI
Heerkens Marc	ISB
Hefti Esther	Staatskanzlei Kanton Zürich
Kessler Thomas	Temet
Kunz Marc	Berner Fachhochschule, TI
Laube-Rosenpflanzer Annett	Berner Fachhochschule, TI
Leimer Bojan	Berner Fachhochschule, TI
Spichiger Andreas	Berner Fachhochschule, FBW
	eCH Fachgruppe IAM

V2.0:
Ronny Bernold, BFH FBW, ronny.bernold@bfh.ch
Gerhard Hassenstein, BFH TI, gerhard.hassenstein@bfh.ch
Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch
Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch
Martin Topfel, BFH FBW, martin.topfel@bfh.ch
eCH Fachgruppe IAM

V1.0:
Willy Müller, ISB, willy.mueller@isb.admin.ch
Hans Häni, AFT TG

Anhang C – Abkürzungen

AP	Attribute Provider
C2G	Citizen to Government
CP	Credential Provider
CSP	Credential Service Provider
eIDAS	electronic IDentification, Authentication and trust Services
IAM	Identity und Access Management
IdP	Identity Provider
IoT	Internet of Things
ISMS	Infomationssicherheitsmanagementsystem
ITIL	IT-Service-Management
LB	Leistungsbezüger
LE	Leistungserbringer
OIDC	OpenID Connect
PIN	Personal Identification Number
PUF	Physical Unclonalbe Function
RA	Registrierungsstelle / Registration Authority
RP	Relying Party
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SoD	Segregation of Duties
SSO	Single Sign-On
TLS	Transport Layer Security
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Anhang D – Glossar

In diesem Standard werden ausschliesslich die Begriffe aus dem eCH-Standard eCH-0219 V1.0 [1] verwendet.

Anhang E – Änderungen gegenüber Version 2.00

Der vorliegende Standard basiert auf dem Gestaltungsprinzip eCH-0107 v2.00. Es sind in der Überarbeitung aber wesentliche neue Erkenntnisse und Konzepte eingeflossen.

So wurde eCH-0107 in der Version 3.0 in wesentlichen Teilen überarbeitet.

Nachfolgend werden die generellen Änderungen aufgeführt und auf die jeweiligen Inhalte in eCH-0107 Version 2.00 verwiesen.

Grundsätzliches:

- *Der Aufbau der Kapitel wurde nicht grundsätzlich geändert, sondern die einzelnen Kapitel wurden überarbeitet.*
- *V2.0 beschränkt sich konsequent auf das organisationsübergreifendes IAM.*

Das Glossar von V2.0 enthielt viele Begriffe aus dem IAM, die nicht im Dokument verwendet wurde. Um in Zukunft eine einheitliche Terminologie bei allen IAM-Standards verwenden zu können, wurde dieses Glossar in einen eigenen Standard (eCH-0219 [1]) ausgelagert. Im Dokument selbst werden nur einige zum Verständnis notwendigen die verwendeten Begriffe zitiert.

Einleitung [eCH-0107 V2.0 Kapitel 2]

- *Die Einleitung wurde komplett überarbeitet und auf föderiertes IAM in organisationsübergreifenden Kontext fokussiert.*

Kapitel 3 Akteure und Stakeholder [eCH-0107 V2.0 Kapitel 3]

- *Es wird neu zwischen Stakeholder und Akteure im IAM unterschieden; während die Stakeholder den motivierenden Aspekt beschreiben, sind die verschiedenen Akteure die Ausführenden der Prozesse aus Kapitel 6. Die Beziehungen zwischen Stakeholdern und Akteuren werden beschrieben.*

Kapitel 4 Anforderungen

- *Die Designprinzipien und allgemeine Anforderungen an ein föderiertes IAM-System wurden überarbeitet und durch neue Erkenntnisse (z. B. aus eCH-0168* [13]*, eCH-0174* [14]*, eCH-0170* [11]*) ergänzt. Sie wurden neu strukturiert, klassifiziert und begründet.*
- *Die Anforderungen der verschiedenen Stakeholder wurden überarbeitet, erweitert, begründet.*

Kapitel 5 Informationsarchitektur [eCH-0107 v2.00 Kapitel 5]

- *Das Informationsmodell wurde erweitert. Dabei wurden die Ergänzungen aus dem eCH-Standard eCH-0170* [11] *übernommen und in das vorhandene Modell übernommen.*
- *Eine weitere Ergänzung betrifft das Subjekt, das neu zusätzlich **Dinge** umschliesst, sowie die Unterscheidung von handelnden und nicht handelnden Organisationen. Auch die Delegation von Rechten wird neu adressiert.*

Kapitel 6 Prozesse [eCH-0107 v2.00 Kapitel 5]

- *Die Prozesse wurden aktualisiert, ergänzt und konkretisiert. Neu sind die feinere Unterteilung der Prozesse und die Hinzunahme der unterstützenden Prozesse (Kapitel 6.5). Alle Prozesse wurden durch Anforderungen aus Kapitel 4 motiviert.*

Kapitel 7 IAM-Services [eCH-0107 v2.00 Kapitel 6]

- *Die Geschäftsservices wurden in IAM-Services umbenannt.*
- *Die IAM-Services wurden wesentlich überarbeitet und auf föderiertes IAM ausgelegt.*
- *Für alle IAM-Services wurden die Schnittstellen definiert.*
- *Die IAM-Services wurden jeweils zu einem Prozess zugeordnet.*
- *Kapitel 7.5 wurde aufgrund der Aktualisierung der Prozesse in Kapitel 6.1 komplett überarbeitet.*

Kapitel 8 IAM für das IoT [neu]

- *Das Kapitel adressiert die Anforderungen und Auswirkungen des IoT auf die Gestaltungsprinzipien der Identitäts- und Zugriffsverwaltung (IAM).*

Kapitel 9 Privacy [neu]

- Dieses Kapitel beschreibt Anforderungen zum Schutz der Privatsphäre des Subjektes und Richtlinien zur Verwaltung und Verarbeitung von subjektbezogenen Daten.

Kapitel 10 Identity Federation Modells [eCH-0107 v2.00 Kapitel 6]

- Die Bilder im Kapitel angepasst. Die Beschreibungen wurden minimal aktualisiert.

Anhang F – Abbildungsverzeichnis

Anhang G - Tabellenverzeichnis